

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004202

International filing date: 10 March 2005 (10.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-106339
Filing date: 31 March 2004 (31.03.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

14. 3. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 3 月 3 1 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 1 0 6 3 3 9

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号
The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

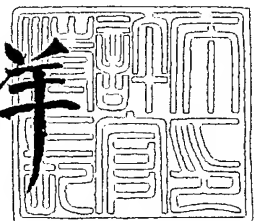
J P 2 0 0 4 - 1 0 6 3 3 9

出 願 人
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 4 月 2 1 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 2048160113
【あて先】 特許庁長官殿
【国際特許分類】 H04N 7/16
G06F 7/14
G06F 12/00
G06F 15/177 682

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 東 吾紀男

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 岡本 隆一

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 村上 弘規

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 徳田 克己

【特許出願人】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社

【代理人】
【識別番号】 100109210
【弁理士】
【氏名又は名称】 新居 広守

【手数料の表示】
【予納台帳番号】 049515
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0213583

【書類名】 特許請求の範囲**【請求項 1】**

ユーザに対して、コンテンツの利用許諾を与えるためのライセンスを配信する送出装置と、前記ライセンスを取得し、前記ライセンスに基づきコンテンツをセキュアに利用する端末装置と、から構成されるデジタル権利管理システムであって、
前記送出装置は、前記ライセンスを生成するライセンス生成手段と、
前記ライセンスに、IDを付与するライセンスID付与手段と、
前記ライセンスに、前記ライセンスの取得が可能な期限を示すライセンス取得期限を付与するライセンス取得期限付与手段と、
前記ライセンスを前記端末装置に送出するライセンス送出手段と、
を備え、
前記端末装置は、
前記ライセンスを取得するライセンス取得手段と、
少なくとも、前記ライセンスに付加された前記ライセンスIDと、前記ライセンス取得期限と、を含むライセンス取得履歴を記録するライセンス取得履歴記録手段と、
前記ライセンスの取得時に、取得する前記ライセンスのライセンスIDと同一のライセンスIDが、前記ライセンス取得履歴記録手段が保持する前記ライセンス取得履歴に存在する場合に、前記ライセンスの取得を抑制するライセンス取得抑制手段と、
を備え、
前記ライセンス取得履歴記録手段は、少なくとも前記ライセンス取得期限までは、前記ライセンスIDと前記ライセンス取得期限からなる前記ライセンス取得履歴を保持することを特徴とするデジタル権利管理システム。

【請求項 2】

前記端末装置は、さらに、前記ライセンスのフォーマットを変換するライセンス変換手段を備え、
前記ライセンス変換手段は、前記ライセンスの取得時に、前記ライセンスのフォーマットを変換し、前記ライセンスのフォーマットを変換した履歴を、前記ライセンス取得履歴として前記ライセンス取得履歴記録手段に送信することを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 3】

前記送出装置は、さらに、前記ライセンスを暗号化して暗号化ライセンスを生成するライセンス暗号化手段を備え、
前記端末装置は、さらに、前記暗号化ライセンスを復号して復号済みライセンスを生成するライセンス復号手段と、
前記復号済みライセンスを再暗号化するライセンス再暗号化手段と
を備え、
前記ライセンス再暗号化手段は、前記送出装置が送出する前記暗号化ライセンスとは異なる暗号鍵を用いて、前記復号済みライセンスを再暗号化することにより、前記ライセンスを前記端末装置にバインドすることを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 4】

前記ライセンスは、デジタル放送のECM (Entitlement Control Message) あるいはACI (Account Control Message) あるいはEMM (Entitlement Management Message) のいずれかに設定される、または、前記ライセンスは、ECMあるいはACIあるいはEMMのいずれかそのものであることを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 5】

前記ライセンス取得期限は、前記ライセンスの有効期限であることを特徴とする請求項 1 または請求項 4 記載のデジタル権利管理システム。

【請求項 6】

前記ライセンス取得期限は、前記ライセンスの有効期限とは別に設定されることを特徴とする請求項 1 または請求項 4 記載のデジタル権利管理システム。

【請求項 7】

前記送出装置は、さらに、前記ライセンスに前記ライセンス取得期限を付与するか否かを決定する前記ライセンス取得期限付与決定手段を備え、

前記ライセンス取得履歴記録手段は、前記ライセンス取得期限付与決定手段が前記ライセンスに前記ライセンス取得期限を設定しない場合には、前記ライセンス取得履歴の前記ライセンス取得期限を生成する

ことを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 8】

前記送出装置は、さらに、前記ライセンスにサービス種別を設定するサービス種別設定手段を備え、

前記ライセンス取得履歴記録手段は、前記ライセンスに設定された前記サービス種別に基づき、ライセンス取得履歴を記録するか否かを決定する

ことを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 9】

前記ライセンス取得履歴記録手段は、前記サービス種別がデジタル放送におけるフラット／ティア契約であるライセンスのみを、ライセンス取得履歴として記録する

ことを特徴とする請求項 8 記載のデジタル権利管理システム。

【請求項 10】

前記送出装置は、さらに、前記ライセンスにサービス種別を設定するサービス種別設定手段を備え、

前記ライセンス取得履歴記録手段は、さらに、前記サービス種別を前記ライセンス取得履歴として記録する

ことを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 11】

前記送出装置は、さらに、前記ライセンスにライセンス取得条件を付与するライセンス取得条件付与手段を備え、

前記ライセンス取得抑制手段は、前記ライセンスに付与された前記ライセンス取得条件に基づき、前記ライセンスの取得を制御する

ことを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 12】

前記端末装置は、さらに、ハードウェア的に耐タンパ化されたセキュリティモジュールを備え、

前記セキュリティモジュールが、前記ライセンス取得履歴記録手段および前記ライセンス取得抑制手段および前記ライセンス取得手段の少なくとも 1 つを備える

ことを特徴とする請求項 1 記載のデジタル権利管理システム。

【請求項 13】

前記端末装置は、さらに、少なくとも前記ライセンス取得履歴の一部を前記端末装置に蓄積するライセンス取得履歴蓄積手段を備え、

前記セキュリティモジュールは、さらに、少なくとも前記ライセンス取得履歴蓄積手段に蓄積した前記ライセンス取得履歴を含むデータのハッシュ値を保持するハッシュ値保持手段を備える

ことを特徴とする請求項 12 記載のデジタル権利管理システム。

【請求項 14】

前記端末装置は、前記端末装置を特定可能な端末装置 ID を保持する第 1 の端末装置 ID 保持手段を備え、

前記セキュリティモジュールは、前記端末装置 ID を保持する第 2 の端末装置 ID 保持手段を備え、

前記第 2 の端末装置 I D 保持手段は、前記ライセンス取得手段が最初に前記ライセンスを取得した時点で挿入されている前記端末装置の前記第 1 の端末装置 I D 保持手段から取得した前記端末装置 I D を保持し、

前記ライセンス取得抑制手段は、前記ライセンスを取得する場合に、前記第 1 の端末装置 I D 保持手段から取得した端末装置 I D と、前記第 2 の端末装置 I D 保持手段に保持する端末装置 I D とを比較し、一致しない場合には、前記端末装置でのさらなる前記ライセンスの取得を抑制する

ことを特徴とする請求項 1 2 記載のデジタル権利管理システム。

【請求項 1 5】

前記端末装置は、前記端末装置を特定可能な端末装置 I D を保持する第 1 の端末装置 I D 保持手段を備え、

前記セキュリティモジュールは、前記ライセンス取得履歴蓄積手段に前記ライセンス取得履歴を蓄積した場合に、前記ライセンス取得履歴を蓄積した前記端末装置の第 1 の端末装置 I D 保持手段から取得する前記端末装置 I D を保持する第 2 の端末装置 I D 保持手段を備え、

前記ライセンス取得抑制手段は、前記ライセンスを取得する場合に、前記第 1 の端末装置 I D 保持手段から取得した端末装置 I D と、前記第 2 の端末装置 I D 保持手段に保持する端末装置 I D とを比較し、一致しない場合には、前記端末装置でのさらなる前記ライセンスの取得を抑制する

ことを特徴とする請求項 1 3 記載のデジタル権利管理システム。

【請求項 1 6】

前記端末装置は、さらに、ユーザに警告などのメッセージを提示するためのメッセージ提示手段を備え、

前記メッセージ提示手段は、前記ライセンス取得抑制手段が前記ライセンスの取得を抑制した場合に、少なくとも、前記ライセンスの取得ができない旨、あるいは、前記ライセンスの取得ができない理由をメッセージとしてユーザに提示する

ことを特徴とする請求項 1 記載のデジタル権利管理システム。

【書類名】明細書

【発明の名称】デジタル権利管理システム

【技術分野】

【0001】

本発明は、デジタル放送、インターネットなどで配信される映像、音楽などのデジタルコンテンツの利用権利を管理し、ユーザが利用権利に基づき端末装置でデジタルコンテンツを利用するシステムに関し、特に、端末装置におけるデジタルコンテンツの利用権利の取得を、事業者の意図に従って確実に制御することが可能なシステムに関する。

【背景技術】

【0002】

近年、音楽、映像などのデジタルコンテンツ（以下、コンテンツと記述）を、デジタル放送、デジタルCATV（Cable Television）、インターネットなどを通じて、放送局から端末装置に配信し、端末装置においてコンテンツを利用することが可能なコンテンツ配信サービスが実用化の段階を迎えている。このコンテンツ配信サービスでは、コンテンツの著作権を保護し、悪意あるユーザなどによるコンテンツの不正利用を防止するため、著作権保護技術が用いられるのが一般的である。著作権保護技術とは、具体的には、暗号技術や認証技術などを用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。著作権保護技術を用いることにより、放送局などのコンテンツプロバイダ、サービスプロバイダが、端末装置におけるユーザのコンテンツ利用をセキュアに制御することが可能となる。

【0003】

ところで、近年、HDD（Hard Disk Drive）などの大容量蓄積手段を有する端末装置において、配信されたコンテンツを一旦端末装置に蓄積し、ユーザが好きなときに蓄積されたコンテンツを視聴するという、ユーザ利便性の高い利用形態が検討されている。日本におけるデジタル放送の規格化団体であるARIB（Association of Radio Industries and Businesses）においては、大容量蓄積機能を活用するデジタル放送方式として、サーバ型放送方式が規格化されており、特にコンテンツの蓄積時における再生を限定するため方式として、限定再生方式が策定されている。なお、サーバ型放送方式における限定再生方式については、ARIB STD-B25 4.1版が詳しい。

【0004】

このような蓄積機能を有する端末装置においては、コンテンツとともに、コンテンツの利用権利であるライセンスも端末装置に蓄積されるため、ライセンスを自由に複製することが可能である。その結果、同一のコンテンツについて複数のライセンスが無制限に取得できてしまう可能性が生ずる。もちろん、通常ライセンスは暗号化が施された状態で配信されるため、どのユーザであっても自由に利用できるわけではないが、少なくとも放送局との視聴契約を行ったユーザについては、特に月ぎめ契約（サブスクリプション）の場合などは、ライセンスを無制限に取得することが容易に可能となる。

【0005】

特許文献1では、このような課題と類似の課題を解決するデジタル権利管理システムとして、記録媒体に書き出すコンテンツの数を制限するため、記録媒体に書き出すコンテンツIDをリストで管理する手法が開示されている。また、この手法では、コンテンツIDを記載したリストサイズの無制限な増加を防止するため、リストサイズの上限も管理しており、リストのサイズが上限に達した場合には、リストへの登録日時の古いレコードの順にコンテンツIDを削除するようになっている。

【特許文献1】特開2004-5526号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかしながら、従来のデジタル権利管理システムでは、登録日時の古い順に、リストからレコードを削除する方式であるので、リストへのライセンスIDの登録・削除の繰り返しにより、結果的に複数の同一ライセンスを無制限に不正に取得されてしまう可能性があり、ユーザの取得可能なライセンス数を制限したいという事業者の権利を十分に保護することができない、という課題があった。

【0007】

本発明は、こうした従来の問題点を解決するものであり、デジタル放送などにおいてライセンスを配信する場合に、ユーザによる無制限なライセンス取得を防止するとともに、リストのサイズの増大を防止することが可能なデジタル権利管理システムを提供することを目的としている。

【課題を解決するための手段】

【0008】

上記目的を達成するために、本発明に関わるデジタル権利管理システムは、ユーザに対して、コンテンツの利用許諾を与えるためのライセンスを配信する送出装置と、前記ライセンスを取得し、前記ライセンスに基づきコンテンツをセキュアに利用する端末装置とから構成されるデジタル権利管理システムであって、前記送出装置は、前記ライセンスを生成するライセンス生成手段と、前記ライセンスに、IDを付与するライセンスID付与手段と、前記ライセンスに、前記ライセンスの取得が可能な期限を示すライセンス取得期限を付与するライセンス取得期限付与手段と、前記ライセンスを前記端末装置に送出するライセンス送出手段とを備え、前記端末装置は、前記ライセンスを取得するライセンス取得手段と、少なくとも、前記ライセンスに付加された前記ライセンスIDと、前記ライセンス取得期限と、を含むライセンス取得履歴を記録するライセンス取得履歴記録手段と、前記ライセンスの取得時に、取得する前記ライセンスのライセンスIDと同一のライセンスIDが、前記ライセンス取得履歴記録手段が保持する前記ライセンス取得履歴に存在する場合には、前記ライセンスの取得を抑制するライセンス取得抑制手段とを備え、前記ライセンス取得履歴記録手段は、少なくとも前記ライセンス取得期限までは、前記ライセンスIDと前記ライセンス取得期限からなる前記ライセンス取得履歴を保持することを特徴とする。

【0009】

本構成によって、ユーザによる不正なライセンス取得を防止するとともに、リストのサイズの増大を防止することが可能となる。

【発明の効果】

【0010】

本発明によれば、端末装置で取得したライセンスのIDと有効期限とを、ライセンスの取得履歴として管理し、少なくともライセンスの取得期限までライセンス取得履歴を保持しておくことにより、無制限なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立することが可能となる。

【発明を実施するための最良の形態】

【0011】

以下、本発明における実施の形態について、図面を用いて詳細に説明する。

図1は、本発明における実施の形態に関わる、デジタル権利管理システムを用いたコンテンツ配信システム1の全体の概略構成を示す図である。

【0012】

このコンテンツ配信システム1は、デジタル放送を通じて放送局に設置された送出装置から送出される暗号化コンテンツを、セキュアに利用制御を行いつつ、ユーザが端末装置において利用することが可能なシステムであって、コンテンツやコンテンツのライセンスなどを配信する放送局101と、コンテンツを利用する端末装置102と、端末装置102とともにコンテンツの利用に用いるICカード103と、これらを相互に接続するデジタル放送104、および、通信ネットワーク105とから構成されている。

【0013】

なお、端末装置 1 0 2 は複数あって良いが、図 1 では簡単のため、1 つの端末装置 1 0 2 のみをその代表として示している。

放送局 1 0 1 は、暗号化されたコンテンツ（以下、暗号化コンテンツ）や、暗号化コンテンツを復号するための暗号鍵などを配信する送出装置などを有する。

【0 0 1 4】

端末装置 1 0 2 は、デジタル放送 1 0 4 や通信ネットワーク 1 0 5 などから暗号化コンテンツを受信するとともに、暗号化コンテンツを復号するためのライセンスを受信し、暗号化コンテンツを復号してコンテンツを利用するための装置である。また、端末装置 1 0 2 は、IC カード 1 0 3 を挿入するインタフェースを有しており、高いセキュリティを必要とする処理については、IC カード 1 0 3 と連携することにより処理を実行する。

【0 0 1 5】

IC カード 1 0 3 は、耐タンパ化されたハードウェアモジュールである。具体的には、IC カード 1 0 3 は、国内デジタル放送の標準 C A S が実装された B - C A S カードのような高度なセキュリティを有するカードや、SD (Secure Digital) カードにセキュリティプロセッサが搭載されたようなモジュールなどがあげられる。

【0 0 1 6】

デジタル放送 1 0 4 は、BS (Broadcasting Satellite) デジタル放送、CS (Communication Satellite) デジタル放送、地上デジタル放送などの無線によるデジタル放送や、デジタル C A T V などの有線によるデジタル放送である。

【0 0 1 7】

通信ネットワーク 1 0 5 は、放送局 1 0 1 と端末装置 1 0 2 とを相互に接続するネットワークである。例えば、通信ネットワーク 1 0 5 は、ADSL (Asymmetric Digital Subscriber Line)、FTTH (Fiber To The Home)、双方向デジタル C A T V、IEEE 8 0 2 . 1 1 g などの高速インターネット網である。

【0 0 1 8】

なお、放送局 1 0 1 および端末装置 1 0 2 の構成については、後で図を用いて詳細に説明する。

ここで、サーバ型放送方式における限定再生方式の暗号スキームについて、図 2 を用いて説明する。

【0 0 1 9】

図 2 において、コンテンツや暗号鍵を送出する送信側 2 0 0 と、コンテンツや暗号鍵を受信する受信側 2 5 0 に分けて説明する。

送信側 2 0 0 において、コンテンツは、スクランブル鍵 K s 2 0 1 と呼ばれる暗号鍵によってスクランブル、すなわち、暗号化 (2 0 2) される。コンテンツのスクランブルについては、MPEG-2 トランスポートストリーム (Transport Stream、以下、TS と記述) のパケット単位で、TS パケットのペイロード部をスクランブルする。また、スクランブル鍵 K s 2 0 1 は、不正受信に対するセキュリティ向上のため、数秒おきに変更される時変鍵である。

【0 0 2 0】

また、コンテンツをスクランブルするスクランブル鍵 K s 2 0 1 は、悪意あるユーザなどによる不正な傍受を防止するため、ワーク鍵 K w 2 0 3 を用いて暗号化 (2 0 4) される。ワーク鍵 K w 2 0 3 は、従来の一般的な限定受信方式で用いられている放送事業者毎の契約単位、グループ単位に割り当てられる暗号鍵であり、ワーク鍵 K w 2 0 3 自体のセキュリティを確保するため、数ヶ月～数年の期間で更新されるのが一般的である。少なくともスクランブル鍵 K s 2 0 1 を含み、コンテンツに関連する情報を送信するためのデータ構造は、ECM (Entitlement Control Message) と呼ばれ、MPEG-2 Systems (IEC/ISO 13818-1) のプライベートセクションとして構成される。ワーク鍵 K w 2 0 3 で暗号化された ECM は、ECM-Kw

と呼ばれ、放送コンテンツのリアルタイム視聴において利用する。

【0021】

また、スクランブル鍵 $K_s 201$ は、コンテンツ鍵 $K_c 205$ でも暗号化 (204) される。コンテンツ鍵 $K_c 205$ は、コンテンツ単位に割り当てられる暗号鍵であり、 $ECM-K_w$ と同様、 $MPEG-2 Systems$ のプライベートセクションとして構成される。少なくともスクランブル鍵 $K_s 201$ を含む ECM を、コンテンツ鍵 $K_c 205$ で暗号化したものを $ECM-K_c$ と呼び、放送コンテンツの蓄積視聴 (サーバ型放送方式における $Type I$ コンテンツ) において利用する。

【0022】

さらに、コンテンツ鍵 $K_c 205$ についても、悪意あるユーザなどによる不正な傍受を防止するため、ワーク鍵 $K_w 203$ で暗号化 (206) される。コンテンツ鍵 $K_c 205$ を含み、ワーク鍵 $K_w 203$ で暗号化された ECM を K_c 伝送用 ECM と呼び、放送コンテンツの蓄積視聴において利用する。 K_c 伝送用 ECM は、 $ECM-K_w$ 、および、 $ECM-K_c$ と同様に、 $MPEG-2 Systems$ のプライベートセクションとして構成されるものである。

【0023】

$ECM-K_w$ や K_c 伝送用 ECM を暗号化するワーク鍵 $K_w 203$ は、コンテンツの利用に先立って送信側 200 と受信側 250 とで共有しておく必要があるため、 EMM ($Entitlement Management Message$) と呼ばれるデータ構造を利用して両者で共有する。このとき、スクランブル鍵 $K_s 201$ やコンテンツ鍵 $K_c 205$ と同様、盗聴防止のため、マスタ鍵 $K_m 207$ と呼ばれる端末装置 102 固有の暗号鍵で暗号化 (208) する。このマスタ鍵 $K_m 207$ についても、送信側 200 と受信側 250 で予め共有しておく必要があるが、受信側 250 のマスタ鍵 $K_m 252$ は、端末装置 102 のセキュアな部分や、セキュリティモジュールと呼ばれるハードウェア的に耐タンパ化されたモジュールなどに出荷時などに予め書き込まれることで設定される。

【0024】

なお、 $ECM-K_w$ 、 $ECM-K_c$ 、 K_c 伝送用 ECM 、 EMM のデータ構造の例については、後で図を用いて詳細に説明する。

また、本暗号スキームにおいて、端末装置 102 では、マスタ鍵 $K_m 207$ 、ワーク鍵 $K_m 203$ など、特にセキュリティを必要とする情報の管理および処理を、ICカードで行うようにするようによい。

【0025】

また、本暗号スキームで使用する暗号アルゴリズムとしては、 AES ($Advanced Encryption Standard$) などの共通鍵暗号方式が用いられる。

また、ワーク鍵 $K_w 203$ については、送信側 200 と受信側 250 との間で SAC ($Secure Authenticated Channel$) を確立し、通信ネットワーク 105 を介してワーク鍵 $K_w 203$ を共有するようによい。

【0026】

以上のように生成された暗号化コンテンツ、 $ECM-K_w$ 、 $ECM-K_c$ 、 K_c 伝送用 ECM 、および、 EMM は、 $MPEG-2 TS$ パケット化され、必要に応じて PSI ($Program Specific Information$) / SI ($Service Information$) などのデータと多重化 (209) された後、受信側 250 に送信される。

【0027】

一方、受信側 250 では、送信側 200 から送出された $MPEG-2 TS$ パケットを受信し、これらを分離 (251) して、暗号化コンテンツ、 $ECM-K_w$ 、 $ECM-K_c$ 、 K_c 伝送用 ECM 、および、 EMM を取得する。

【0028】

この暗号化された EMM は、受信側 250 で予め保持しているマスタ鍵 $K_m 252$ を用いて復号 (253) し、ワーク鍵 $K_w 203$ を取得する。このワーク鍵 $K_w 203$ は、受

信側 250 の不揮発性メモリなどで保持される。

【0029】

コンテンツをリアルタイム視聴する場合、ECM-Kw を取得して、ワーク鍵 Kw 203 により暗号化された ECM-Kw を復号 (255) して、スクランブル鍵 Ks 201 を取得する。スクランブル鍵 Ks 201 によって暗号化コンテンツを復号 (256) して、コンテンツを利用することが可能となる。

【0030】

一方、コンテンツを蓄積視聴する場合、図示しない蓄積部に記録された暗号化コンテンツ、ECM-Kc、Kc 伝送用 ECM を読み出す。Kc 伝送用 ECM については、送信側 200 からは繰り返し送出されるが、受信側 250 では 1 回だけ取得すれば良い。なお、ECM-Kw は、リアルタイム視聴時のみで使用されるため、受信側 250 では蓄積されない。

【0031】

リアルタイム視聴の場合において説明した方法で取得したワーク鍵 Kw 203 を用いて、暗号化された Kc 伝送用 ECM を復号 (254) して、コンテンツ鍵 Kc 205 を取得する。これによりコンテンツ鍵 Kc 205 により ECM-Kc を復号 (255) し、暗号化コンテンツを復号 (256) して、コンテンツを利用することが可能となる。

【0032】

以上、図 2 を用いて、サーバ型放送方式の限定再生方式の暗号スキームについて説明した。以降、本発明における実施の形態では、図 2 で説明した暗号スキームに基づくデジタル権利管理システムについての説明を行う。

【0033】

このようなコンテンツ配信システム 1 において、デジタル放送 104 を通じて、コンテンツ (番組)、ライセンスが配信され、端末装置 102 において、コンテンツ、ライセンスを HDD などに蓄積し、ライセンスに基づきコンテンツを利用する処理を、図 3 ~ 図 2 の図面を用いて詳細に説明する。

【0034】

図 3 は、図 1 に示す放送局 101 の構成を示す機能ブロック図である。

放送局 101 は、契約情報を管理する契約情報管理 DB 301 と、ワーク鍵を管理するワーク鍵 DB 302 と、コンテンツに関連する属性情報を管理するコンテンツ属性情報 DB 303 と、コンテンツ毎に割り当てられるコンテンツ鍵を管理するコンテンツ鍵 DB 304 と、映像、音声などのコンテンツを管理するコンテンツ DB 305 と、端末装置 102 とのインタフェースを提供する通信部 306 と、ユーザの契約情報を管理する契約処理部 307 と、端末装置 102 毎の個別情報を生成する EMM 生成部 308 と、EMM を暗号化する EMM 暗号化部 309 と、全端末装置 102 に共通な情報を生成する ECM 生成部 310 と、ECM を暗号化する ECM 暗号化部 311 と、コンテンツをエンコードするコンテンツ符号化部 312 と、MP EG-2 TS を多重化する多重化部 313 と、映像、音声などの TS パケットを暗号化するコンテンツ暗号化部 314 と、TS 化されたコンテンツを送出するコンテンツ送出部 315 とで構成されている。

【0035】

契約情報管理 DB 301 は、ユーザのコンテンツの視聴契約に関する情報を管理するためのデータベースである。具体的には、契約情報管理 DB 301 は、図 4 に示すように、IC カード 103 毎の視聴契約に関連する情報や、マスタ鍵 Km 207 を一元管理する契約情報管理テーブル 400 を有する。契約情報管理 DB 301 は、主として、EMM 生成部 308 が、端末装置 102 毎に視聴契約情報を配信するための EMM を生成する際に参照する。

【0036】

カード ID 401 は、端末装置 102 に挿入する IC カード 103 を一意に識別し、契約処理を行った IC カード 103 に対して EMM 900 を送出するための宛て先となる情報である。

【0037】

ティア契約ID402は、放送局101が提供するサービスに対する月極め契約（サブスクリプション）の識別をするためのIDであり、一種の契約形態を示している。例えば、スポーツに関するコンテンツを視聴できる「スポーツコンテンツパック」、映画コンテンツを視聴できる「映画コンテンツパック」などがあげられる。

【0038】

PPV契約ID403は、放送局101が提供するサービスに対するペイ・パー・ビューの視聴契約を識別するためのIDであり、ティア契約ID908と同様、一種の契約形態を示している。

【0039】

有効期限404は、放送局101との契約期間を示すものであり、有効期限904までは、当該放送局101のコンテンツを利用することが可能となる。

蓄積暗号鍵Km'405は、端末装置102において、コンテンツやライセンス（ECMなど）をHDDなどに蓄積する場合に、コンテンツやライセンスを取得した端末装置102、すなわち、ICカード103に、コンテンツやライセンスをバインドする際に用いる。

【0040】

マスタ鍵Km406は、ICカード103固有の暗号鍵であり、ECMを暗号化する場合に用いる。ICカード103では出荷時に埋め込まれる。

例えば、図4では、カードID401が「CARD-ID-1」なるICカード103は、ティア契約ID402が「TIERCONT-ID-1」、PPV契約ID403が「PPVCONT-ID-1」であるサービスに加入しており、有効期限404が「2004/4/1~2005/3/31」であり、蓄積暗号鍵Km'405が「0x1111・・・1111」、マスタ鍵Km406が「0x1111・・・1111」であることを示している。

【0041】

ワーク鍵DB302は、ユーザが事業者と視聴契約を行った場合に送出するECMを暗号化する鍵を管理するためのデータベースであって、ワーク鍵管理テーブル500を有する。ワーク鍵DB302は、ECM-Kw、Kc伝送用ECMを暗号化する際に、ワーク鍵Kw203を提供したりする場合に用いられる。

【0042】

具体的には、ワーク鍵DB302は、図5に示すように、ワーク鍵ID501、ワーク鍵Kw502、ワーク鍵利用開始日503の組を管理するワーク鍵管理テーブル500を管理する。

【0043】

例えば、図5では、ワーク鍵ID501「WK-ID-1」に対応するワーク鍵Kw502が「0x123・・・cdf」であり、ワーク鍵Kw502の利用開始日を示すワーク鍵利用開始日503が「2003/11/24」であることを示している。また、ワーク鍵ID501は、暗号化されたECMにおいて、暗号化に用いたワーク鍵Kw203を特定するために用いられる情報であり、ECM-Kwのワーク鍵ID1104や、Kc伝送用ECMのワーク鍵ID1004に設定される。

【0044】

コンテンツ属性情報DB303は、コンテンツの利用条件や、当該コンテンツを視聴可能な契約の種類など、コンテンツ利用に関する種々の情報を管理するためのデータベースである。具体的には、コンテンツ属性情報DB303は、図6に示すように、コンテンツ配信システム1内でコンテンツを一意に特定するためのコンテンツID601と、コンテンツ配信システム1内でライセンスを一意に特定するためのライセンスID602と、利用条件603と、契約情報604と、ライセンス変換期限605とを有するコンテンツ属性情報管理テーブル600を備えている。

【0045】

例えば、コンテンツID601が「CONTENT-ID-1」、ライセンスID602が「LICENSE-ID-1」であるコンテンツは、利用条件603が「有効期限1ヶ月」、契約情報604が「TIERCONT-ID-1」、ライセンス変換期限605が「2004/4/30」であることから、放送局101と「TIERCONT-ID-1」なるサービスを契約し、「2004/4/30」までにライセンスを取得する処理を行った場合、コンテンツを蓄積してから1ヶ月間は当該コンテンツが再生可能であることを示している。なお、ライセンス変換期限605に関わるライセンス変換処理については、端末装置102の構成について説明する際に、詳細に説明する。

【0046】

また、コンテンツID601が「CONTENT-ID-2」なるコンテンツについては、契約情報604が「TIERCONT-ID-1、TIERCONT-ID-2」であることから、このコンテンツを視聴するためには、放送局101と「TIERCONT-ID-1」または「TIERCONT-ID-2」の少なくともどちらかのサービスを契約していることが必要となる。また、コンテンツID601が「CONTENT-ID-4」なるコンテンツについては、契約情報604が「PPVCONT-ID-1」であることから、このコンテンツがPPVコンテンツであることが示されている。

【0047】

コンテンツ鍵DB304は、端末装置102に蓄積されたコンテンツを利用するためのライセンス毎（すなわち、コンテンツ毎）に割り当てられる暗号鍵を管理するデータベースである。

【0048】

具体的には、コンテンツ鍵DB304は、コンテンツ配信システム1においてコンテンツをユニークに識別するための識別子であるコンテンツID701、コンテンツ配信システム1においてライセンスをユニークに識別するための識別子であるライセンスID702、ライセンスID702に設定するコンテンツ鍵Kc703から構成されるコンテンツ鍵管理テーブル700を有する。

【0049】

例えば、図7では、図7では、コンテンツ701が「CONTENT-ID-1」に対応するライセンスID702が、「LICENSE-ID-1」であり、これらに対応するコンテンツ鍵Kc703が、「0x123...cdf」であることを示している。

【0050】

コンテンツDB305は、コンテンツを蓄積するためのデータベースである。具体的には、コンテンツDB305は、図8に示すように、コンテンツ配信システム1内でコンテンツを一意に特定するためのコンテンツID801と、コンテンツの名前を示すコンテンツ名称802と、コンテンツをデジタル放送で配信する日時を示す放送日時803と、コンテンツ毎のコンテンツDB305におけるファイルの位置を示すファイル名804とを有するコンテンツ管理テーブル800を備えている。

【0051】

例えば、コンテンツID801が「CONTENT-ID-1」のコンテンツは、コンテンツ名称802が「マンドースポーツ」であり、放送日時803が「2004/4/8 21:00:00」、コンテンツDB305におけるファイル名804はURI (Uniform Resource Identifier) が「/SPORT/.../MSPORTS.VC」（「...」はURIの一部が省略されていることを示している）であることを示している。

【0052】

なお、コンテンツ管理テーブル800は、アナログVCR (Video Cassette Recorder) であってもよいし、コンテンツ管理テーブル800に代わり、ライブ放送（生放送）などを撮影するビデオカメラなどであっても良い。

【0053】

通信部306は、通信ネットワーク105を通じて、端末装置102と通信するための

部である。

契約処理部 307 は、端末装置 102 からの視聴契約の申し込みを処理する部である。

【0054】

具体的には、契約処理部 307 は、Web ブラウザなどを通じて放送局 101 との視聴契約を受け付け、ユーザ（端末装置 102）に対する視聴契約情報を、契約情報管理 DB 301 に登録する。

【0055】

EMM 生成部 308 は、ワーク鍵 Kw 203 やユーザの契約情報などを含む EMM を生成する部である。

具体的には、EMM 生成部 308 は、主として新規契約や契約変更が行われたユーザ（端末装置 102、すなわち、IC カード 103）に対して、契約情報管理 DB 301 から当該ユーザの契約内容であるティア契約 ID 402、PPV 契約 ID 403、有効期限 404 などを読み出し、EMM に設定する。

【0056】

ここで、図 9 を用いて、EMM のデータ構造についての詳細な説明を行う。

図 9 は、主としてワーク鍵 Kw 201 やユーザ毎（IC カード 103 毎）の情報を伝送する EMM のデータ構造の一例を示す図である。

【0057】

図 9 に示した EMM 900 は、カード ID 902、事業者 ID 903、有効期限 904、ワーク鍵 ID 905、ワーク鍵 Kw 906、蓄積暗号鍵 Km' 907、ティア契約 ID 908、PPV 契約 ID 909、改ざん検出 910 とから構成されている。また、MP EG-2 Systems のプライベートセクション形式でトランスポートストリームに多重化するため、セクションヘッダ 901、セクションテラ（誤り検出）911 が付加されている。EMM 900 に示したデータの大部分は、IC カード 103 に蓄積され、管理される。

【0058】

カード ID 902 は、コンテンツ配信システム 1 において、端末装置 102 に挿入する IC カード 103 を一意に識別し、契約処理を行った IC カード 103 に対して EMM 900 を送出するための宛て先となる情報である。

【0059】

事業者 ID 903 は、コンテンツ配信システム 1 において、サービスを提供する事業者を識別するコードであって、後述するワーク鍵 ID 905 とともに参照される。

有効期限 904 は、放送局 101 との契約期間を示すものであり、有効期限 904 までは、当該放送局 101 のコンテンツを利用することが可能となる。

【0060】

ワーク鍵 ID 905 は、ECM を暗号化するワーク鍵 Kw 203 を識別するための情報であり、IC カード 103 で暗号化された ECM を復号する際には、ワーク鍵 ID 905 と同様の情報が ECM の非暗号化部分に設定されるので、ワーク鍵 ID 905 を参照することにより、どのワーク鍵 Kw 203 を用いて暗号化された ECM を復号すれば良いかを判別することができる。

【0061】

ワーク鍵 Kw 906 は、放送局 101 との契約に対してユーザに与えられる暗号化であり、IC カード 103 で暗号化された ECM-Kw、および、Kc 伝送用 ECM を復号する際に用いる。

【0062】

蓄積暗号鍵 Km' 907 は、端末装置 102 において、コンテンツやライセンス（ECM など）を HDD などに蓄積する場合に、コンテンツやライセンスを取得した端末装置 102、すなわち、IC カード 103 に、コンテンツやライセンスをバインドする際に用いる。

【0063】

ティア契約ID908は、放送局101が提供するサービスに対する月極め契約（サブスクリプション）の識別をするためのIDであり、「標準パック」、「プレミアムパック」などの放送局101との契約形態を示している。

【0064】

PPV契約ID909は、放送局101が提供するサービスに対するペイ・パー・ビューの視聴契約を識別するためのIDであり、ティア契約ID908と同様、一種の契約形態を示している。

【0065】

改ざん検出910は、暗号化したEMM900の改ざんを検出するためのハッシュ値が設定される。ハッシュアルゴリズムは、AESのCBCモードで暗号化した結果であるMAC（Message Authentication Code）や、SHA-256などを用いる。

【0066】

なお、ここでは、ティア契約、PPV契約については、ティア契約ID908、PPV契約ID909をそのままEMM900に設定する場合の例を説明したが、それぞれのIDをビットマップなどで表現したものをEMM900で配信し、伝送すべき情報量とICカード103での保持すべき情報量を削減するようにしても良い。

【0067】

また、ここでは、ワーク鍵Kw203は事業者毎に割り当てる場合の例を説明したが、ティア契約ID毎などの契約毎にワーク鍵Kw203を割り当てるようにしても良い。

以上、図9を用いて、EMM900のデータ構造についての詳細な説明を行った。

【0068】

EMM暗号化部309は、AESなどを用いて、EMM生成部308で生成したEMM900を暗号化する部である。

具体的には、EMM暗号化部309は、EMM生成部308で生成したEMM900を、契約情報管理DB301から取得したマスタ鍵Km207で暗号化し、多重化部313に送信する。EMM900を暗号化するにあたっては、暗号化モードは、CBC（Cipher Block Chaining）+OFB（Output FeedBack）を用いる。

【0069】

ECM生成部310は、スクランブル鍵Ks201などを含むECMを生成する部である。具体的には、ECM生成部310は、上流システムからの指示により、コンテンツの送出に合わせてECM-Kw、ECM-Kc、Kc伝送用ECMを生成する。ECM-Kw、および、ECM-Kcの生成については、コンテンツのセキュリティを堅固なものとするため、数秒おきにスクランブル鍵Ksを生成して、ECM-Kw、ECM-Kcに設定する。Kc伝送用ECMの生成については、コンテンツ属性情報DB303、および、コンテンツ鍵DB304から、利用条件603やコンテンツ鍵Kc703などを取得して、Kc伝送用ECMに設定する。また、生成したスクランブル鍵Ks201を、コンテンツを暗号化するコンテンツ暗号化部314に送信する。

【0070】

ここで、図10～図11を用いて、ECM-Kw、ECM-Kc、Kc伝送用ECMのデータ構造についての詳細な説明を行う。

図10は、主としてスクランブル鍵Ks201を伝送するECM-KwおよびECM-Kcのデータ構造の一例を示す図である。

【0071】

図10に示したECM-Kw1000、および、ECM-Kc1020は、スクランブル鍵Ks201やコンテンツに関する情報の伝送に用いられる情報であり、事業者ID1002、ワーク鍵ID1003、コンテンツID1004、スクランブル鍵Ks1005、契約判定情報1006、改ざん検出1007とから構成されている。また、MPEG-2 Systemsのプライベートセクション形式でトランスポートストリームに多重化

するため、セクションヘッダ 1001、セクションテラ（誤り検出）1007が付加されている。

【0072】

事業者ID 1002は、コンテンツ配信システム1において、サービスを提供する事業者を識別するコードであって、次に述べるワーク鍵ID 1003とともに参照される。

ワーク鍵ID 1003は、ECMを暗号化するワーク鍵Kw 203を識別するための情報であり、ECMの非暗号化部分に設定される。ICカード103で、暗号化されたECMを復号する場合には、ワーク鍵ID 1003を参照することにより、どのワーク鍵Kw 203を用いてECMを復号すれば良いかを判別することができる。

【0073】

コンテンツID 1004は、コンテンツ配信システム1内でコンテンツに対して一意に割り当てられる識別子であり、コンテンツの識別のために用いる。

スクランブル鍵Ks 1005は、コンテンツのTSパケットのペイロード部を暗号化する暗号鍵である。端末装置102が、数秒おきに更新されるスクランブル鍵Ks 1005を取得するために要する時間を短縮するため、一般的にはスクランブル鍵Ks 1005に複数の暗号鍵を設定する。

【0074】

契約判定情報1006は、当該コンテンツの属性を示す情報であり、端末装置102でコンテンツを視聴する場合に、当該コンテンツを視聴するための契約がなされているかを判定するために用いる。

【0075】

改ざん検出1007は、暗号化されるECMの改ざんを検出するためのハッシュ値が設定される。ハッシュアルゴリズムは、EMM900の場合と同様、AESのCBC-MACや、SHA-256などを用いる。

【0076】

次に、図11は、主として蓄積視聴のためのECM-Kc 1020を復号するためのコンテンツ鍵Kc 205を送送するKc伝送用ECMのデータ構造の一例を示す図である。

図11に示したKc伝送用ECM1100は、コンテンツ鍵Kc 205やコンテンツの利用条件（ライセンス）の伝送に用いられる情報であり、事業者ID 1102、サービスタイプ1103、ワーク鍵ID 1104、契約判定情報1105、ライセンス変換期限1106、ライセンスID 1107、ライセンス有効期限1108、コンテンツ鍵Kc 1109、利用可能回数1110、書き出し可能回数1111、改ざん検出1112とから構成されている。また、ECM-Kc 1000およびECM-Kc 1020と同様に、セクションヘッダ1101、セクションテラ（誤り検出）1113が付加されている。

【0077】

事業者ID 1102、ワーク鍵ID 1104、契約判定情報1105、改ざん検出1112については、ECM-Kc 1000、および、ECM-Kc 1020における事業者ID 1002、ワーク鍵ID 1003、契約判定情報1006、改ざん検出1008の説明と同様であるので、ここでは説明を省略する。

【0078】

サービスタイプ1103は、Kc伝送用ECM1100を含むコンテンツが、ティア契約で視聴可能なコンテンツであるのか、PPV契約であって、別途購入処理を行うことによって視聴可能なコンテンツであるのか、を識別するためのフラグである。本発明の実施の形態においては、ティア契約を「TIERCONT」、PPV契約を「PPVCONT」として、以下の説明を行う。

【0079】

ライセンス変換期限1106は、ICカード103において、Kc伝送用ECM1100を変換して、蓄積視聴用のライセンスを取得する処理の期限を示すものである。ライセンス変換とは、Kc伝送用ECM1100に含まれる情報を用いて、蓄積視聴用のライセンスをフォーマット変換により生成する処理を指す。このライセンス変換期限1106を

経過した場合には、Kc 伝送用 ECM 1 1 0 0 から蓄積視聴に必要なライセンスを取得することはできず、ライセンス変換期限 1 1 0 6 経過後に、別途、通信などを用いて取得する必要がある。

【0 0 8 0】

ライセンス ID 1 1 0 7 は、変換したライセンスをコンテンツ配信システム 1 内で一意に識別するためのコードであり、IC カード 1 0 3 において、ライセンスの変換履歴としても用いる。

【0 0 8 1】

ライセンス有効期限 1 1 0 8 は、当該ライセンスにより、コンテンツを視聴可能な期限を示すものである。

コンテンツ鍵 Kc 1 1 0 9 は、コンテンツ単位で割り当てられる 1 6 バイト長の暗号鍵であり、ライセンスに含まれる暗号鍵である。

【0 0 8 2】

利用可能回数 1 1 1 0 は、当該ライセンスにより、コンテンツを視聴可能な回数を示すものである。

書き出し可能回数 1 1 1 1 は、当該ライセンスにより、コンテンツを蓄積媒体に書き出すことが可能な回数を示すものである。

【0 0 8 3】

なお、ワーク鍵 Kw 2 0 3 で暗号化されたリアルタイム視聴用の ECM-Kc 1 0 0 0 と、コンテンツ鍵 Ks 2 0 5 で暗号化された蓄積視聴用の ECM-Kc 1 0 2 0 のフォーマットは同一であり、暗号化を行う暗号鍵（ワーク鍵 Kw 2 0 3 とコンテンツ鍵 Ks 2 0 5）と、セクションヘッダ 1 0 0 1 に記載されるセクション識別情報（テーブル ID、テーブル ID エクステンションなど）や TS パケットの PID (P a c k e t I D) などが異なる。

【0 0 8 4】

また、ライセンス変換期限 1 1 0 6 を、ライセンス有効期限 1 1 0 8 とは別に設けることによって、端末装置 1 0 2 にコンテンツおよびライセンスを大量に蓄積し、短期の視聴契約を行うことによって、視聴契約期間以外に蓄積した過去のライセンスも含めて、短期間に大量のライセンスを取得されてしまうという課題を解決することができる。この場合には、ライセンス変換期限 1 1 0 6 は、比較的短い期限を設定すると良い。また、この目的のためには、必ずしもライセンス (Kc 伝送用 ECM) 毎にライセンス変換期限 1 1 0 6 を設ける必要はなく、システム固定値として IC カード 1 0 3 などがあらかじめ保持しておくようにしても良い。

【0 0 8 5】

以上、図 1 0 ～図 1 1 を用いて、ECM-Kw 1 0 0 0、ECM-Kc 1 0 2 0、Kc 伝送用 ECM 1 1 0 0 のデータ構造についての詳細な説明を行った。

ECM 暗号化部 3 1 1 は、AES などを用いて、ECM 生成部 3 1 0 で生成した ECM を暗号化する部である。具体的には、ECM 暗号化部 3 1 1 は、ECM 生成部 3 1 0 で生成した ECM-Kw 1 0 0 0、および、Kc 伝送用 ECM 1 1 0 0 を、ワーク鍵 DB 3 0 2 から取得したワーク鍵 Kw 2 0 3 で暗号化する。合わせて、ECM 生成部 3 1 0 で生成した ECM-Kc 1 0 2 0 を、コンテンツ鍵 DB 3 0 4 から取得したコンテンツ鍵 Kc 2 0 5 で暗号化する。各 ECM を暗号化するにあたっては、暗号化モードは、CBC+OFB を用いる。ECM 暗号化部 3 1 1 は、このように暗号化した各 ECM を、多重化部 3 1 3 に送信する。

【0 0 8 6】

コンテンツ符号化部 3 1 2 は、端末装置 1 0 2 に送出するコンテンツをコンテンツ DB 3 0 5 から読み出し、コンテンツを MPEG 形式で符号化する部である。

具体的には、コンテンツ符号化部 3 1 2 は、MPEG ストリームを生成するリアルタイムエンコーダであって、上流システム（例えば、番組運行管理システムなど）の指示により、コンテンツ DB 3 0 5 から映像、音声などを読み出し、映像、音声、データなどの M

PEG-2やMPEG-4のES (Elementary Stream) を生成する。さらに、これらのESを含むPES (Packetized Elementary Stream) パケットを生成し、最後にMPEG-2 TSパケット化して、多重化部313に送出する。

【0087】

多重化部313は、コンテンツ符号化部312から受け取った映像、音声、データなどを含むトランスポートストリームと、ECM暗号化部311から受け取ったECMのトランスポートストリームと、EMM暗号化部309から受け取ったEMM900のトランスポートストリームとを多重化し、多重化されたトランスポートストリームをコンテンツ暗号化部314に送出する部である。具体的には、多重化部313は、コンテンツ符号化部312から受信したTSパケット化されたコンテンツと、ECM暗号化部311から受信したTSパケット化されたECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100と、EMM暗号化部309から受信したTSパケット化されたEMM900とをTS多重化して、端末装置102に送信するための多重化トランスポートストリームを生成する。

【0088】

コンテンツ暗号化部314は、AESなどを用いてコンテンツを暗号化することにより、コンテンツのスクランブルを行う部である。具体的には、コンテンツ暗号化部314は、TSパケットのアダプテーションフィールドを除くペイロード部を、ECM生成部310から取得したスクランブル鍵Ks201を用いて、CBC+OFBモードによって暗号化(スクランブル)する。

【0089】

コンテンツ送出部315は、コンテンツ暗号化部314において暗号化されたTSパケットを、端末装置102に送出する部である。具体的には、コンテンツ送出部315は、コンテンツ暗号化部314から受け取ったトランスポートストリームを、放送波としてネットワーク103を通じて端末装置102に送出する。

【0090】

なお、ここでは、コンテンツDB305に蓄積されたコンテンツを読み出し、コンテンツ符号化部312においてリアルタイムエンコードする場合の例を示したが、あらかじめオフラインでPES (ES) あるいはTSを生成しておき、コンテンツDB305に蓄積しておくことにより、コンテンツ送出時にコンテンツ符号化部312におけるエンコード処理を省略するようにしても良い。

【0091】

以上、図3～図11を用いて、放送局101の構成についての詳細な説明を行った。

一方、図12は、図1に示す端末装置102、および、ICカード103の構成を示す機能ブロック図である。

【0092】

まず、端末装置102を構成する機能ブロックについての説明を行う。

送受信部1201は、デジタル放送104、および、通信ネットワーク105を通じて、放送局101からのコンテンツやライセンスを受信したり、放送局101と通信したりするための部である。

【0093】

分離部1202は、MPEG-2 TSにより多重化された暗号化コンテンツを取得し、コンテンツとECMなどとを分離するための部である。

具体的には、分離部1202は、送受信部1201が受信したトランスポートストリームに含まれるPAT (Program Association Table)、PMT (Program Map Table) などのPSI情報を参照して、コンテンツの映像、音声、データや、ECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100を含むTSパケットのPIDを取得し、コンテンツとECM-Kc1020などとを分離する。コンテンツ蓄積部1203にコンテンツを蓄積する場合には、PAT、P

MTなどのPSI情報から必要な情報を選択してSIT (Selection Information Table)、DIT (Discontinuity Information Table)などのPSI情報の生成を行い、受信したトランスポートストリームを、パーシャルトランスポートストリーム（以下、パーシャルTSと記述する）と呼ばれるストリームを生成する処理を行う。

【0094】

蓄積部1203は、コンテンツやライセンスなどを蓄積するための部である。具体的には、蓄積部1203は、HDDなどの大容量不揮発性記憶媒体であり、分離部1202において受信したトランスポートストリームから生成した、映像、音声などのコンテンツやECM-Kc1020などのライセンスを含むパーシャルTSを蓄積する。

【0095】

蓄積管理部1204は、端末装置102の蓄積部1203に蓄積するコンテンツやライセンスを管理しており、蓄積したコンテンツやライセンスの一覧などをユーザに提示するための情報を有する。

【0096】

コンテンツ復号部1205は、暗号化コンテンツを復号する部である。具体的には、コンテンツ復号部1205は、暗号化されたMPEG-2 TSのコンテンツを取得し、トランスポートストリームに含まれるPAT、PMTなどのPSI情報を参照して、コンテンツの映像、音声、データを含むTSパケットを取得する。そして、ICカード103から取得するスクランブル鍵Ks201でAES暗号化されたTSパケットのペイロード部分を復号する。

【0097】

コンテンツ利用部1206は、ICカード103から取得するスクランブル鍵Ks201とコンテンツの利用条件とを用いて、セキュアにコンテンツの利用を行うための部である。

【0098】

具体的には、コンテンツ利用部1206は、リアルタイム視聴時においては、分離部1202から受け取ったトランスポートストリームからECM-Kw1000のTSパケットを取得し、ECM-Kw1000を再構成する。このようにして得られたECM-Kw1000をワーク鍵Kw203で復号して、コンテンツをデスクランブルするためのスクランブル鍵Ks201を取得し、コンテンツを復号する。一方、蓄積視聴時においては、蓄積部1203から読み出したトランスポートストリームから、Kc伝送用ECM1100をワーク鍵Kw203で復号して、ライセンスを取得する。そして、ライセンスに含まれる利用条件判定を行った上で、コンテンツを利用可能である場合のみ、ライセンスに含まれるコンテンツ鍵Kc205を用いて、ECM-Kc1020を復号して、スクランブル鍵Ks201を取得する。さらに、コンテンツ利用部1206は、図12に図示しないセキュアな計時部を用いて、コンテンツの利用時間などを計時することにより、利用条件に従ったコンテンツの利用を制御する。このような制御のもと、コンテンツ利用部1206は、MPEG-2あるいはMPEG-4の映像、音声、データなどのESをデコードして、図12に示さないモニタなどに出力する。

【0099】

なお、コンテンツの利用を終了した場合に、ICカード103に対して、利用終了通知を通知するようにしても良い。

端末装置102における第1のカードI/F部1207は、端末装置102とICカード103とのインタフェースを提供するための部である。

【0100】

具体的には、第1のカードI/F部1207は、ISO7816-4で規定されているT=0プロトコルやT=1プロトコルを処理し、端末装置102やICカード103の他の機能ブロックとの間で相互にデータをやりとりするための手段を提供するものである。端末装置102とICカード103との通信は、悪意あるユーザなどによる通信の傍受を

防止するため、少なくともセキュリティを要する情報の授受については、端末装置102とICカード103との間で相互認証が行われ、SAC (Secure Authenticated Channel) を確立した上で行われる。

【0101】

ユーザI/F部1208は、端末装置102とユーザとのインタフェースを提供するための部である。

具体的には、ユーザI/F部1208は、BML (Broadcasting Markup Language) ブラウザ、Webブラウザ、レジデントアプリケーションなどのGUI (Graphical User Interface) であり、図12に示さないモニタなどを通じて、ユーザ要求を受け付けたり、ユーザにメッセージを提示したりする。

【0102】

以上、端末装置102を構成する機能ブロックについての説明を行った。

次に、ICカード103を構成する機能ブロックについての説明を行う。

カード情報管理DB1210は、ユーザのコンテンツの視聴契約に関する情報を管理するためのデータベースである。具体的には、カード情報管理DB1210は、全事業者で共通の視聴契約に関連する情報を管理する共通情報テーブル1300と、事業者毎の視聴契約に関する情報を管理する事業者別情報テーブル1400とを有する。

【0103】

カード情報管理DB1210の共通情報テーブル1300は、図13に示すように、カードID1301と、マスタ鍵Km1302と、蓄積暗号鍵Km' 1303とを管理する。

【0104】

カードID1301は、コンテンツ配信システム1内でICカード103を一意に識別するためのIDであり、ICカード103に予め書き込まれて出荷される。

マスタ鍵Km1302は、EMM900を暗号化する場合に用いられるカードID1301固有の暗号鍵であり、カードID1301と同様、ICカード103に予め書き込まれて出荷される。

【0105】

蓄積暗号鍵Km' 1303は、端末装置102の蓄積部1203でライセンスを蓄積する場合に、ライセンスの取得を行ったICカード103にライセンスをバインドするための暗号鍵であり、EMM900の事業者ID903で指定されるIDである。

【0106】

一方、カード情報管理DB1210の事業者別情報テーブル1400は、図14に示すように、事業者ID1401と、ティア契約ID1402と、PPV契約ID1403と、有効期限1404と、ワーク鍵ID1405と、ワーク鍵Kw1406とを管理する。

【0107】

事業者ID1401は、コンテンツ配信システム1内で一意に放送局101を識別するためのIDであり、EMM900の事業者ID903で指定されるIDである。

ティア契約ID1402は、ユーザが放送局101と月極めコンテンツの視聴契約を行ったサービスのIDであり、EMM900のティア契約ID908で指定されるIDである。

【0108】

PPV契約ID1403は、ユーザが放送局101とPPVコンテンツの契約を行ったサービスのIDであり、EMM900のPPV契約ID909で指定されるIDである。

有効期限1404は、放送局101との視聴契約における視聴期限を示すものであり、EMM900の有効期限904で指定される期限である。

【0109】

ワーク鍵ID1405は、コンテンツ配信システム1内で、放送局101から配布されるワーク鍵Kw203を一意に識別するためのIDであり、EMM900のワーク鍵ID

9 0 5 で指定される ID である。但し、ワーク鍵 Kw 2 0 3 の識別については、事業者 ID 1 4 0 1 とワーク鍵 ID 1 4 0 5 との組により、コンテンツ配信システム 1 内でユニークとなることに注意されたい。

【0 1 1 0】

ワーク鍵 Kw 1 4 0 6 は、放送局 1 0 1 から配布されるワーク鍵 Kw 2 0 3 であり、E M M 9 0 0 のワーク鍵 Kw 9 0 6 で指定される 1 6 バイトのバイト列である。

例えば、図 1 4 では、事業者 ID 1 4 0 1 が「SERVICE-ID-1」である事業者との契約内容は、ティア契約 ID 1 4 0 2 が「TIERCONT-ID-1」、PPV 契約 ID 1 4 0 3 が「PPVCONT-ID-1」、有効期限 1 4 0 4 が「2 0 0 4 / 4 / 1 ~ 2 0 0 5 / 3 / 3 1」、ワーク鍵 ID 1 4 0 5 が「KW-ID-1」、ワーク鍵 Kw 1 4 0 6 が「0 x 1 1 1 . . . 1 1 1」であることを示しており、「SERVICE-ID-1」であるコンテンツは、ティアコンテンツ（Kc 伝送用 ECM 1 1 0 0 のサービスタイプ 1 1 0 4 が「TIERCONT」であるコンテンツ）と PPV コンテンツ（Kc 伝送用 ECM 1 1 0 0 のサービスタイプ 1 1 0 4 が「PPVCONT」であるコンテンツ）の両方のコンテンツが視聴可能である。また、事業者 ID 1 4 0 1 が「SERVICE-ID-1 0」である事業者については、ティア契約 ID 1 4 0 2 が「-（未契約）」、PPV 契約 ID 1 4 0 3 が「PPVCONT-ID-1」であることから、「SERVICE-ID-1」であるコンテンツは、ティアコンテンツについては視聴不可であるが、PPV コンテンツに関しては、別途購入処理を行うことによって視聴が可能である。

【0 1 1 1】

なお、ここでは、ワーク鍵 ID 1 4 0 5 とワーク鍵 1 4 0 6 の組は、最新の一组を保持する場合の例を示したが、ワーク鍵の運用を切り替える際のスムーズな移行を行うため、事業者別情報テーブル 1 4 0 0 においては、少なくとも二組のワーク鍵を保持できるようにしておくのが望ましい。

【0 1 1 2】

変換履歴 DB 1 2 1 1 は、ライセンスの変換履歴を蓄積するためのデータベースである。具体的には、変換履歴 DB 1 2 1 1 は、Kc 伝送用 ECM 1 1 0 0 に含まれる情報から、蓄積視聴用のライセンスが無制限に変換されることを防止するため、ライセンスの変換（以下、ライセンス変換と記述）が行われたことを示す変換履歴（Transformation Log、以下、TL と記述）を保持する。

【0 1 1 3】

ここで、変換履歴 DB 1 2 1 1 に蓄積する TL のデータ構造の一例を、図 1 5 を用いて説明する。

TL 1 5 0 0 は、ライセンス変換を行ったライセンスを識別するためのライセンス ID 1 5 0 1 と、ライセンス変換が可能な期間を示すライセンス変換期限 1 5 0 2 との組から構成されており、これらの複数組をリストとして管理している。TL 1 5 0 0 の各レコードは、少なくとも、ライセンス変換期限 1 5 0 2 を経過するまでは保持されるため、一度変換を行ったライセンスについては、さらなるライセンス変換を抑制することができ、その結果、1 つの Kc 伝送用 ECM 1 1 0 0 からは、1 つのライセンスのみを取得することができるので、事業者の権利を確実に保護することができる。

【0 1 1 4】

ライセンス DB 1 2 1 2 は、放送局 1 0 1 から取得したライセンスをセキュアに管理するためのデータベースである。具体的には、ライセンス DB 1 2 1 2 は、放送局 1 0 1 から取得したライセンスを蓄積、管理するとともに、端末装置 1 0 2 の蓄積部 1 2 0 3 などの IC カード 1 0 3 の外部にライセンスを蓄積する場合において、ライセンスの改ざんなどの不正な行為を防止するため、ライセンス DB 1 2 1 2 中のライセンスのハッシュ値を管理する。

【0 1 1 5】

第 2 のカード I / F 部 1 2 1 3 は、端末装置 1 0 2 における第 1 のカード I / F 部 1 2 0 7 と同様の機能ブロックであるため、ここでは説明を省略する。

ECM/EMM復号部1214は、端末装置102から受信した、暗号化されたECM、および、暗号化されたEMM900を復号するための部である。具体的には、ECM/EMM復号部1214は、第2のカードI/F部1213から暗号化ECM-Kw1000、暗号化ECM-Kc1020、暗号化EMM900を受け取り、カード管理情報DB1210から、それぞれに対応するワーク鍵Kw203(1406)、マスタ鍵Km207(1302)を読み出し、また、ライセンスDB1212に保持されているライセンスからコンテンツ鍵Kc205を受け取り、暗号化ECM-Kw1000、暗号化ECM-Kc1020、Kc伝送用ECM1100、暗号化EMM900の暗号を復号する。

【0116】

ECM/EMM処理部1215は、平文のECMやEMMから必要な情報を抽出したり、処理したりするための部である。具体的には、ECM/EMM処理部1215は、ECM/EMM復号部1214から受け取ったECM-Kw1000、ECM-Kc1020、Kc伝送用ECM1100、EMM900を解釈し、カード管理情報DB1210の構築に必要な情報を抽出して記録したり、端末装置102がコンテンツの再生に要するスクランブル鍵Ks201を、ECM-Kw1000やECM-Kc1020から抽出して、端末装置102にレスポンスとして返送したりする。

【0117】

ライセンス変換処理部1216は、放送局101から受信したECMなどに含まれる情報(またはライセンスそのもの)を、蓄積コンテンツの利用を制御するためのライセンスに変換するとともに、変換したライセンスの数を管理するための部である。具体的には、ライセンス変換処理部1216は、放送局101から取得したKc伝送用ECM1100に含まれる情報を、図16に示す蓄積視聴用のライセンスのフォーマットに変換するとともに、変換したライセンスのライセンスIDと有効期限とを管理するための変換履歴であるTL1500を生成、管理する。

【0118】

ここで、ライセンス変換処理部1216が変換するライセンスの構成の一例を、図16を用いて説明する。

ライセンス1600は、コンテンツの利用を許諾する情報であり、ライセンス識別子1601と、ライセンスID1602と、有効期限1603と、再生回数1604と、書き出し回数1605と、コンテンツ鍵Kc1606と、ライセンス1600の改ざんを検出するための改ざん検出1607とから構成されている。

【0119】

ライセンス識別子1601は、コンテンツ配信システム1で利用可能なライセンスを識別するための識別子である。例えば、「SV-DRM LICENSE」のような識別子であり、ライセンス変換処理部1216であらかじめ保持している識別子である。

【0120】

ライセンスID1602は、コンテンツ配信システム1内でライセンスを一意に識別するための識別子である。ライセンスID1602は、Kc伝送用ECM1100のライセンスID1107の値を設定する。

【0121】

有効期限1603は、ライセンス1600が利用可能な期間を示し、利用開始日時および利用終了日時を有する。有効期限1603は、Kc伝送用ECM1100のライセンス有効期限1108の値を設定する。

【0122】

再生回数1604は、コンテンツを再生可能な回数を示し、再生回数が0より大である場合には、再生が可能となる。再生回数1604は、Kc伝送用ECM1100の利用可能回数1110の値を設定する。

【0123】

書き出し回数1605は、DVD(Digital Versatile Disc)やBD(Blu-Ray Disc)などの記録媒体などへのコンテンツの複製回数を示

す。書き出し回数 1605 は、Kc 伝送用 ECM1100 の書き出し可能回数 1111 の値を設定する。

【0124】

コンテンツ鍵 Kc1606 は、ECM-Kc1020 を復号するためのコンテンツ鍵 Kc205 を示す。コンテンツ鍵 Kc205 がバイナリ値で設定され、ECM-Kc1020 を復号する場合に用いる。コンテンツ鍵 Kc1606 は、Kc 伝送用 ECM1100 のコンテンツ鍵 Kc1109 の値を設定する。

【0125】

改ざん検出 1607 は、ライセンス 1600 をハードディスクなどの非セキュアな領域に蓄積する場合に、改ざんの検出を行い、その正当性を確保するためのものであって、ライセンス 1600 の内容が更新される度に、ライセンス 1600 の改ざんを防止したい箇所（典型的には、ライセンス識別子 1601～コンテンツ鍵 Kc1606）についてハッシュ値を計算し、計算結果を管理する。このハッシュ値は、ハード的に耐タンパ化された IC カード 103 の内部で管理する。ハッシュアルゴリズムとしては、例えば、SHA-1 (Secure Hash Algorithm 1) や、SHA-256 などが挙げられる。また、ライセンス 1600 をハードディスクなどの非セキュアな領域に蓄積する場合には、少なくともコンテンツ鍵 Kc1606 の部分は暗号化されて蓄積される。

【0126】

以上、図 16 を用いて、コンテンツ配信システム 1 におけるライセンス 1600 の構成の説明を行った。

ライセンス処理部 1217 は、ライセンスに基づき、コンテンツの利用可否判定をセキュアに行う。

【0127】

具体的には、ライセンス処理部 1217 は、ユーザからライセンスの利用要求を受けた場合に、放送局 101 から取得したライセンスに含まれる利用条件に基づき、コンテンツの利用が可能かどうかを判定する。そして、利用条件がコンテンツの利用を許諾している場合に限り、ECM-Kc1020 を復号するためのコンテンツ鍵 Kc205 を ECM/EMM 復号部 1214 に渡す、という処理を行う。

【0128】

例えば、ライセンス処理部 1217 は、ライセンス 1600 に設定された有効期限 1603 を参照し、コンテンツが利用可能かどうかを判定する。端末装置 102 に保持している、図 12 には図示しないセキュアな計時部により提供される現在時刻を参照し、現在時刻が有効期限 1603 内である場合は、コンテンツの再生が可能である、というような判定処理を行う。

【0129】

以上、図 12～図 16 を用いて、端末装置 102 および IC カード 103 についての詳細な構成の説明を行った。

さて、以上のように構成された端末装置 102 および IC カード 103 において、ユーザが放送局 101 との視聴契約を行い、放送局 101 の配信装置からコンテンツおよびライセンスを取得して、端末装置 102 に蓄積し、端末装置 102 においてコンテンツを利用するという一連の動作を、図 17～図 22 に示すフローチャートを用いて説明する。

【0130】

なお、図 17～図 22 に示すフローチャートにおいて、ユーザが PPV コンテンツを利用する場合には、コンテンツの購入処理が必要であるが、これらの処理については本発明の主眼ではないため、以下では説明を省略する。

【0131】

最初に、端末装置 102 において、ユーザが放送局 101 と視聴契約を行う動作を、図 17 に示すフローチャートを用いて説明する。

まず端末装置 102 において、ユーザが、ユーザ I/F 部 1208 が提供する GUI により、放送局 101 との視聴契約を行う（ステップ S1701）。

【0132】

具体的には、ユーザが、ユーザI/F部1208が提供するGUIによって、放送局101が提供するティア契約、または、PPV契約の視聴契約のうち所望の契約を選択すると、ユーザI/F部1208は、対応する契約を識別するためのID（以下、契約IDと記述）を、ICカード103のカードID1301などとともに送受信部1201に送信する。送受信部1201は、放送局101とSSL（Secure Sockets Layer）などを用いてSACを確立し、受け取った契約IDとカードID1301とを放送局101に送信する。なお、ユーザI/F部1208は、Webブラウザなどによってあらかじめ契約IDを取得済みであるものとする。また、カードID1301についても、ICカード103の挿入時などにあらかじめ取得済みであるものとする。

【0133】

放送局101は、端末装置102からの視聴契約の申し込みを受け付ける（ステップS1702）。

具体的には、放送局101の通信部306は、端末装置102から契約IDなどを受信すると、契約IDを契約処理部307に渡す。

【0134】

放送局101は、端末装置102から受信した契約IDに基づき、契約処理を行い、ユーザの契約に関する情報をデータベースに登録する（ステップS1703）。

具体的には、契約処理部307は、必要に応じて、クレジットカード番号や銀行口座番号などを用いて課金処理を行い、契約情報管理DB301にユーザの視聴契約情報を登録する。このとき契約処理部307は、合わせて、ICカード103固有の蓄積暗号鍵Km'305を生成し、ICカード103固有のマスタ鍵Km306とともに、契約情報管理DB301に登録する。

【0135】

なお、ICカード103毎に固有のマスタ鍵Km306については、鍵管理センタなどからあらかじめ取得しておくものとする。

放送局101のEMM生成部308は、視聴契約を行ったユーザに対するEMM900を生成する（ステップS1704）。

【0136】

具体的には、EMM生成部308は、顧客管理システムなどの上位のシステムからの随時または一日一回などのEMM送出指示に基づき、契約情報管理DB301の契約情報管理テーブル400から、EMM900を送出すべきカードID401のティア契約ID402～蓄積暗号鍵Km'405を抽出し、該当カードID401宛てのEMM900を生成する。EMM生成部308は、生成したEMM900をEMM暗号化部309に送信する。

【0137】

放送局101のEMM暗号化部309は、生成したEMM900に対応するマスタ鍵で、EMM900を暗号化する（ステップS1705）。

具体的には、EMM暗号化部309は、EMM生成部308から受け取ったEMM900のカードID902を参照して、契約情報管理DB301の契約情報管理テーブル400から、カードID401が合致するICカード103のマスタ鍵Km406を読み出す。このマスタ鍵Km406を用いて、EMM900の必要部分をAESで暗号化する。EMM暗号化部309は、暗号化したEMM900を多重化部313に送信する。

【0138】

放送局101は、暗号化したEMM900を、コンテンツなどと多重化し、端末装置102に送出する（ステップS1706）。

具体的には、多重化部313は、EMM暗号化部309から受け取ったEMM900と、コンテンツ符号化部312などから受け取ったコンテンツなどをTSパケット化した後、TS多重化する。その後、コンテンツ暗号化部314において、コンテンツの必要部分がスクランブルされ、コンテンツ送出部315が、放送波としてEMM900を含むT

Sを端末装置102に送出する。

【0139】

端末装置102は、自己宛てのEMM900を受信する（ステップS1707）。

具体的には、端末装置102の送受信部1201および分離部1202は、事前にICカード103から取得したカードIDを用いて、受信したEMM900をフィルタリングし、自己宛てのEMM900を抽出する。

【0140】

端末装置102の第1のカードI/F部1207は、受信したEMM900をICカード103に送出する（ステップS1708）。

ICカード103の第2のカードI/F部1213は、端末装置102の第1のカードI/F部1207からEMM900を受信する（ステップS1709）。

【0141】

ICカード103は、ICカード103内で、EMM900に含まれる情報を管理する（ステップS1710）。

具体的には、第2のカードI/F部1213が受信したEMM900を、ECM/EMM復号部1214に送信する。ECM/EMM復号部1214は、EMM900のカードID902が自身のICカード103が保持するカードIDと一致することを確認した上で、カード管理情報DB1210の共通情報テーブル1300からマスタ鍵Km1302を読み出し、EMM900のカードID902を復号する。復号後、EMM900の改ざん検出910を用いて、暗号化EMM900が正しく復号できたことを確認する。改ざんが発見された場合は、当該EMM900の処理を中断する。ECM/EMM復号部1214は、復号したEMM900をECM/EMM処理部1215に渡す。ECM/EMM処理部1215は、受け取ったEMM900を解釈し、必要な情報をカード管理情報DB1210に蓄積し、図13および図14に示した、共通情報テーブル1300および事業者別情報テーブル1400を構築する。

【0142】

なお、ここでは、端末装置102が通信ネットワーク105を通じて、放送局101に対して視聴契約の申し込みを行う場合の例を示したが、電話やハガキなどのオフラインによる視聴契約の申し込みであっても良い。

【0143】

次に、放送局101における送出装置が、コンテンツを送出する動作を、図18に示すフローチャートを用いて説明する。

まず、ECM生成部310は、コンテンツ送出指示を受信すると、コンテンツ送出開始に先立ち、Kc伝送用ECM1100を生成する（ステップS1801）。

【0144】

具体的には、ECM生成部310は、番組運行管理装置などの上流システムからのコンテンツ送出指示、すなわち、ECM生成指示をトリガとして、コンテンツ単位の暗号鍵を有するKc伝送用ECM1100を生成するため、コンテンツ属性情報DB303およびコンテンツ鍵DB304を参照して、ライセンスID602、利用条件603、コンテンツ鍵Kc703などを読み出す。読み出した情報から、図11に示したKc伝送用ECM1100を生成する。ECM生成部310は、生成したKc伝送用ECM1100を、ECM暗号化部311に送信する。

【0145】

ECM暗号化部311は、ワーク鍵Kw203でKc伝送用ECM1100を暗号化する（ステップS1802）。

具体的には、ECM暗号化部311は、ワーク鍵DB302のワーク鍵管理テーブル500のワーク鍵利用開始日503を参照して、現在使用中のワーク鍵Kw203を特定する。特定したワーク鍵ID501とワーク鍵Kw502を読み出し、ECM生成部310から受信したKc伝送用ECM1100の必要部分をAESでCBC+OFBモードによる暗号化を施す。合わせて、Kc伝送用ECM1100のワーク鍵ID1104に、ワー

ク鍵 ID 5 0 1 を設定する。ECM 暗号化部 3 1 1 は、暗号化した K c 伝送用 ECM 1 1 0 0 を多重化部 3 1 3 に送信する。

【0 1 4 6】

コンテンツ符号化部 3 1 2 は、コンテンツの読み出し、送出を開始し、コンテンツ送出中はコンテンツの送出が完了したか否かを監視する（ステップ S 1 8 0 3）。

具体的には、コンテンツ符号化部 3 1 2 は、ステップ S 1 8 0 1 において、ECM 生成部 3 1 0 が上流システムから受信したコンテンツ送出指示と同じ指示を受けて、コンテンツ DB 3 0 5 のコンテンツ管理テーブル 8 0 0 から該当コンテンツを読み出し、コンテンツを MPEG エンコードによりコンテンツの TS を生成する。生成した TS を多重化部 3 1 3 に送信するとともに、コンテンツ DB 3 0 5 からのコンテンツの読み出し、および、多重化部 3 1 3 へのコンテンツの送信が完了したか否かを監視する。

【0 1 4 7】

ステップ S 1 8 0 3 において、NO である場合、すなわち、コンテンツの送信が完了していない場合は、ステップ S 1 8 0 4 を実行する。

ステップ S 1 8 0 3 において、YES である場合、すなわち、コンテンツの送信が完了した場合には、本コンテンツ送出処理を終了する。

【0 1 4 8】

ECM 生成部 3 1 0 は、コンテンツの送出開始に伴い、コンテンツをスクランブルするためのスクランブル鍵 K s 2 0 1 を生成する（ステップ S 1 8 0 4）。

具体的には、ECM 生成部 3 1 0 は、数秒おきに更新されるスクランブル鍵 K s 2 0 1 を順次生成して、生成したスクランブル鍵 K s 2 0 1 をコンテンツ暗号化部 3 1 4 に逐次送信する処理を行う。

【0 1 4 9】

ECM 生成部 3 1 0 は、コンテンツ属性情報から ECM を生成する（ステップ S 1 8 0 5）。

具体的には、コンテンツの送出に合わせて、コンテンツ属性情報 DB 3 0 3 のコンテンツ属性情報管理テーブル 6 0 0 の契約情報 6 0 4 などを読み出し、ECM-K w 1 0 0 0、ECM-K c 1 0 2 0 を生成する。ECM 生成部 3 1 0 は、生成した ECM-K w 1 0 0 0、ECM-K c 1 0 2 0 を、ECM 暗号化部 3 1 1 に送信する。

【0 1 5 0】

ECM 暗号化部 3 1 1 は、ワーク鍵 K w 2 0 3 で ECM-K w を暗号化する（ステップ S 1 8 0 6）。

具体的には、ECM 暗号化部 3 1 1 は、ワーク鍵 K w 2 0 3 による K c 伝送用 ECM 1 1 0 0 の暗号化と同様の方法で、ワーク鍵 DB 3 0 2 のワーク鍵管理テーブル 5 0 0 のワーク鍵利用開始日 5 0 3 を参照して、現在使用中のワーク鍵 K w 2 0 3 を特定し、ワーク鍵 K w 5 0 2 で ECM-K w 1 0 0 0 を AES で暗号化する。ECM 暗号化部 3 1 1 は、暗号化した ECM-K w 1 0 0 0 を多重化部 3 1 3 に送信する。

【0 1 5 1】

ECM 暗号化部 3 1 1 は、コンテンツ鍵 K c 2 0 5 で ECM-K c を暗号化する（ステップ S 1 8 0 6）。

具体的には、ECM 暗号化部 3 1 1 は、コンテンツ鍵 DB 3 0 4 のコンテンツ鍵管理テーブル 7 0 0 を参照して、送出するコンテンツとコンテンツ ID 7 0 1 およびライセンス 7 0 2 が一致するレコードのコンテンツ鍵 K c 7 0 3 を読み出す。ここで、送出するコンテンツのコンテンツ ID とライセンス ID は、上流システムからのコンテンツ送出指示の際に、上流システムなどから取得済みであるとする。読み出したコンテンツ鍵 K c 7 0 3 を用いて、ECM 生成部 3 1 0 から受信した K c 伝送用 ECM 1 1 0 0 の必要部分を AES で CBC+OFB モードによる暗号化を施す。ECM 暗号化部 3 1 1 は、暗号化した ECM-K c 1 0 2 0 を多重化部 3 1 3 に送信する。

【0 1 5 2】

コンテンツ暗号化部 3 1 4 は、コンテンツや ECM が多重化された TS をスクランブル

する (ステップ S1808)。

具体的には、コンテンツ暗号化部 314 は、多重化部 313 においてコンテンツの TS や ECM-Kw1000、ECM-Kc1020、Kc 伝送用 ECM1100 などの TS を多重化した TS のうち、映像、音声、データなどのコンテンツの TS パケットを選択して、AES の CBC+OFB モードで TS パケットのペイロード部分をスクランブルする。

【0153】

コンテンツ送出部 315 は、暗号化された TS を送出する (ステップ S1809)。

具体的には、コンテンツ送出部 315 は、コンテンツ暗号化部 314 においてスクランブルされた TS を、放送波として端末装置 102 に送出する。

【0154】

なお、ここでは、コンテンツの送出開始に合わせて、スクランブル鍵 Ks201、すなわち、ECM-Kw1000、ECM-Kc1020 の送出を行う場合の例を示したが、端末装置 102 において、コンテンツの先頭から確実にデスクランブル可能となるように、コンテンツの送出開始に先立って ECM-Kw1000、ECM-Kc1020 を多重、送出することが望ましい。

【0155】

以上、図 18 を用いて、放送局 101 によるコンテンツの送出処理についての詳細な説明を終了する。

次に、端末装置 102 が、デジタル放送 104 からコンテンツを受信し、蓄積部 1203 に蓄積する動作を、図 19～図 21 に示すフローチャート等を用いて説明する。

【0156】

図 19 は、端末装置 102 および IC カード 103 におけるコンテンツ受信およびライセンス変換処理を示すフローチャートである。ただし、本処理において、IC カード 103 におけるライセンス変換可否判定処理については、別途、図 21 に示すフローチャートを用いて説明する。

【0157】

まず、端末装置 102 における蓄積管理部 1204 は、蓄積部 1203 に蓄積するコンテンツの蓄積状況を監視し、コンテンツ蓄積が終了しているか否かを確認する (ステップ S1901)。

【0158】

具体的には、蓄積管理部 1204 は、ユーザから指定されたサーバ型放送 Type I コンテンツをチューニングし、パーシャル TS として蓄積部 1203 に順次蓄積する。蓄積処理の間、PSI/SI (Program Specific Information / Service Information) などを参照しながら、当該コンテンツを蓄積完了したか否かを監視する。

【0159】

ステップ S1901 において、YES である場合、すなわち、コンテンツの蓄積が未完了である場合には、ステップ S1902 を実行する。

ステップ S1901 において、NO である場合、すなわち、コンテンツの蓄積が完了した場合には、本コンテンツ蓄積処理を終了する。

【0160】

分離部 1202 は、Kc 伝送用 ECM1100 を取得したか否かを判断する (ステップ S1902)。

具体的には、分離部 1202 は、受信した TS の PAT、PMT などを参照し、Kc 伝送用 ECM の PID が付与された TS パケットから Kc 伝送用 ECM1100 を再構成するが、1つのコンテンツ蓄積において、少なくとも 1 回取得すれば良い Kc 伝送用 ECM1100 を取得したか否かを監視する。

【0161】

ステップ S1902 において、YES である場合、すなわち、Kc 伝送用 ECM1100

0を未取得である場合には、ステップS1903を実行する。

ステップS1902において、NOである場合、すなわち、Kc伝送用ECM1100を取得済みである場合には、ステップS1912を実行する。

【0162】

分離部1202は、Kc伝送用ECMを分離し、ICカード103に送信する（ステップS1903）。

具体的には、分離部1202は、ステップS1902の処理において再構成したKc伝送用ECM1100を取得して、第1のカードI/F部1207を通じて、ICカード103に送信する。

【0163】

ICカード103は、受信したKc伝送用ECM1100を変換しても良いか否かを判定する（ステップS1904）。

具体的には、ICカード103の第2のカードI/F部1213は、端末装置102の第1のカードI/F部1207が送信した、暗号化されたKc伝送用ECM1100を受信し、暗号復号処理の後、ライセンス変換処理部1216は、ICカード103内部に蓄積した変換履歴DB1211を用いて、ライセンス変換処理を行ってもよいか否かの判定処理を実行する。なお、本ライセンス変換可否判定処理の詳細については、後で図21を用いて説明するので、ここでは詳細な説明は行わない。

【0164】

ICカード103のライセンス変換処理部1216は、ライセンス変換可否判定処理の結果、ライセンス変換が許可されているか否かを確認する（ステップS1905）。

ステップS1905において、YESである場合、すなわち、ライセンス変換が許可されている場合には、ステップS1906を実行する。

【0165】

ステップS1905において、NOである場合、すなわち、ライセンス変換が許可されていない場合には、ステップS1910を実行する。

ライセンス変換処理部1216は、Kc伝送用ECM1100をライセンス変換し、蓄積視聴用のライセンス1600を生成する（ステップS1906）。

【0166】

具体的には、ライセンス変換処理部1216は、Kc伝送用ECM1100に含まれるライセンスID1107、ライセンス有効期限1108などを取得して、図16に示すようなライセンス1600を生成する。

【0167】

ライセンス変換処理部1216は、変換したライセンスがティアコンテンツであるか、PPVコンテンツであるかを判定する（ステップS1907）。

具体的には、ライセンス変換処理部1216は、Kc伝送用ECM1100のサービスタイプ1103を参照して、サービスタイプ1103が「TEIRCONT」（ティアコンテンツ）であるか、「PPVCONT」（PPVコンテンツ）であるかを判断する。

【0168】

ステップS1907において、YESである場合、すなわち、ティアコンテンツである場合には、ステップS1908を実行する。

ステップS1907において、NOである場合、すなわち、PPVコンテンツである場合には、ライセンス変換履歴を記録する必要がないので、ステップS1908を実行せず、ステップS1909を実行する。ただし、PPVコンテンツのライセンス1600は、購入処理を経て初めて利用可能になるライセンスであるので、例えば、ライセンス変換直後には、ライセンス1600と合わせて、当該ライセンスが未購入であることを示すフラグを保持するようにし、購入処理後にフラグを削除することにより、当該ライセンスが購入済みであることを示す、といった処理が必要である。

【0169】

ライセンス変換処理部1216は、当該ライセンスの変換履歴を記録する（ステップS

1908)。

具体的には、ライセンス変換処理部1216は、変換履歴DB1211に蓄積されているTL1500のライセンスID1501とライセンス変換期限1502に、Kc伝送用ECM1100のライセンスID1107とライセンス変換期限1106を追加する。

【0170】

ライセンス処理部1217は、変換したライセンスをライセンスDB1212に蓄積する(ステップS1909)。

第2のカードI/F部1213は、端末装置102に対して、Kc伝送用ECM1100によるライセンス変換要求に対するレスポンスを送信する(ステップS1910)。

【0171】

具体的には、第2のカードI/F部1213は、当該コンテンツのライセンス変換が許可されており、ライセンス変換が完了したか、あるいは、当該コンテンツのライセンス変換が許可されていない、または、ライセンス変換に失敗した、などのレスポンスメッセージを生成して、端末装置102に送信する。

【0172】

なお、ステップS1905において、NOである場合のように、当該コンテンツのライセンス変換が許可されていない場合には、図20に示すようなメッセージをユーザに提示する。

【0173】

図20は、ユーザI/F部1208がユーザに提示するウォーニングメッセージの一例を示す図である。モニタ2001に表示されているメッセージ2002は、ユーザがICカード103において、コンテンツ「マンドースポーツ」のライセンスIDに対応するライセンスを既にライセンス変換し、取得しているため、これ以上は取得できない旨を示している。

【0174】

第1のカードI/F部1207は、ICカード103からのレスポンスを受信する(ステップS1911)。

具体的には、第1のカードI/F部1207は、ICカード103の第2のカードI/F部1213から、Kc伝送用ECM1100の送信に対するライセンス変換結果のレスポンスを受信する。

【0175】

端末装置102の蓄積管理部1204は、コンテンツを蓄積部1203に蓄積する処理を行う(ステップS1912)。

具体的には、蓄積管理部1204は、コンテンツ、ECM-Kc1020、Kc伝送用ECM1100などのTSパケットを、順次蓄積部1203に蓄積するとともに、合わせて、PMTなどから生成したSIT、DITも蓄積する。なお、何らかの原因によりICカード103でのライセンス変換処理に失敗した場合でも、後で再度ライセンス変換を試みることができるように、コンテンツやECM-Kc1020、Kc伝送用ECM1100の蓄積処理は継続する。

【0176】

以上、図19を用いて、端末装置102におけるコンテンツ蓄積処理についての説明を行った。

次に、ICカード103でのライセンス変換可否判定処理について、図21を用いて詳細に説明する。

【0177】

まず、ICカードのECM/EMM復号部1214は、カード管理情報DB1210を参照して、Kc伝送用ECM1100を復号するためのワーク鍵Kw203が存在するかどうかを判定する(ステップS2101)。

【0178】

具体的には、ECM/EMM復号部1214は、カード管理情報DB1210の事業者

別情報テーブル1400を参照して、Kc伝送用ECM1100の事業者ID1102と、事業者ID1401が一致する事業者IDのレコードを検索して、ワーク鍵Kw1406を読み出す。このとき、端末装置102からKc伝送用ECM1100と一緒に取得した現在時刻が、有効期限1404を超過していたり、Kc伝送用ECM1100のワーク鍵ID1104と事業者別情報テーブル1400のワーク鍵ID1405が一致しない場合などには、ワーク鍵Kw203が存在しないものとして処理する。

【0179】

ステップS2101において、YESである場合、すなわち、ワーク鍵Kw1406が存在する場合には、ステップS2102を実行する。

ステップS2101において、NOである場合、すなわち、ワーク鍵Kw1406が存在しない場合には、ステップS2111を実行する。

【0180】

ECM/EMM復号部1214は、ワーク鍵Kw1406でKc伝送用ECM1100を復号する（ステップS2102）。

具体的には、ECM/EMM復号部1214は、ステップS2101で取得したワーク鍵Kw1406で、AESによりKc伝送用ECM1100の暗号化部を復号し、Kc伝送用ECM1100の改ざん検出1110により、Kc伝送用ECM1100が改ざんされていないかを確認する。万一、Kc伝送用ECM1100が改ざんされていることが検出された場合には、ライセンス変換は許可できないので、ステップS2111を実行して、本処理を終了する（図21には図示せず）。

【0181】

ECM/EMM処理部1215は、ICカード103が、当該コンテンツを視聴するための契約を有しているか否かを判定する（ステップS2103）。

具体的には、ECM/EMM処理部1215は、Kc伝送用ECM1100の契約判定情報1105と、カード管理情報DB1210の事業者別情報テーブル1400のティア契約ID1402またはPPV契約ID1403を比較して、いずれかのIDが一致するか否かの判定処理を行う。

【0182】

ステップS2103において、YESである場合、すなわち、いずれかのIDが一致する場合には、ステップS2104を実行する。

ステップS2103において、NOである場合、すなわち、いずれのIDも一致しない場合には、ステップS2111を実行する。

【0183】

ライセンス変換処理部1216は、Kc伝送用ECM1100がライセンス変換の期限内であるかどうかを判定する（ステップS2104）

具体的には、ライセンス変換処理部1216は、Kc伝送用ECM1100のライセンス変換期限1106を参照して、端末装置102からKc伝送用ECM1100といっしょに取得した現在時刻と比較することにより、当該Kc伝送用ECM1100がライセンス変換期限内であるか否かを判定する。

【0184】

ステップS2104において、YESである場合、すなわち、ライセンス変換期限1106が現在時刻よりも新である場合には、ライセンス変換期限内であると判定し、ステップS2105を実行する。

【0185】

ステップS2104において、NOである場合、すなわち、ライセンス変換期限1106が現在時刻よりも旧である場合には、ライセンス変換期限外であると判定し、ステップS2111を実行する。

【0186】

ライセンス変換処理部1216は、変換履歴DB1211を参照して、該当ライセンスIDの変換履歴を検索する（ステップS2105）。

具体的には、ライセンス変換処理部1216は、変換履歴DB1211のTL1500を参照し、Kc伝送用ECM1100のライセンスID1107と一致するライセンスID1501のレコードを検索する。

【0187】

ライセンス変換処理部1216は、該当ライセンスIDの変換履歴が存在するか否かを判定する(ステップS2106)。

具体的には、ライセンス変換処理部1216は、ステップS2105の検索結果を参照し、Kc伝送用ECM1100のライセンスID1107とTL1500のライセンスID1501が一致するレコードが存在するか否かを確認する。

【0188】

ステップS2106において、YESである場合、すなわち、該当ライセンスIDの変換履歴が存在しない場合には、ステップS2107を実行する。

ステップS2106において、NOである場合、すなわち、該当ライセンスIDの変換履歴が存在する場合には、ステップS2111を実行する。

【0189】

ライセンス変換処理部1216は、TL1500に空きレコードまたは有効期限を超過したレコードが存在するか否かを検索する(ステップS2107)。

具体的には、ライセンス変換処理部1216は、新たにライセンス変換を行うライセンスIDを追記するレコードを発見するため、TL1500を参照して、空きレコードを検索する。空きレコードが存在しない場合は、TL1500のライセンス変換期限1502と、端末装置102からKc伝送用ECM1100と一緒に取得した現在時刻を比較し、ライセンス変換期限1502が現在時刻より新であるレコードを検索する。

【0190】

ライセンス変換処理部1216は、変換履歴DB1211に空きレコードもしくはライセンス変換期限を超過しているレコードが存在するか否かを判定する(ステップS2108)。

【0191】

具体的には、ライセンス変換処理部1216は、ステップS2107の検索結果を参照し、TL1500に空きレコードをもしくはライセンス変換期限1502を超過しているレコードが存在するか否かを判定する。

【0192】

ステップS2108において、YESである場合、すなわち、空きレコードまたはライセンス変換期限1502を超過しているレコードが存在する場合には、ステップS2109を実行する。

【0193】

ステップS2108において、NOである場合、すなわち、空きレコードまたはライセンス変換期限1502を超過しているレコードが存在しない場合には、これ以上ライセンス変換を実行することはできないため、ステップS2111を実行する。

【0194】

ライセンス変換処理部1216は、ステップS2108で判定した結果に基づき、空きレコードがない場合には、ライセンス変換期限1502を超過したレコードを削除し、新たなライセンスID1501の追加をできるようにする(ステップS2109)。

【0195】

ライセンス変換処理部1216は、当該Kc伝送用ECM1100のライセンスを変換を許可と判定し、本ライセンス変換可否判定処理を終了する(ステップS2110)。

ライセンス変換処理部1216は、当該Kc伝送用ECM1100のライセンスを変換は不許可と判定し、本ライセンス変換可否判定処理を終了する(ステップS2111)。

【0196】

以上、図19～図21を用いて、コンテンツ蓄積時の端末装置102およびICカード103の処理の詳細について説明を行った。

最後に、端末装置102が、蓄積部1203のコンテンツを蓄積視聴する動作を、図2に示すフローチャートを用いて説明する。

【0197】

まず、ユーザが視聴したい蓄積コンテンツのライセンスIDを指定すると、端末装置102は、ICカード103に対してコンテンツ鍵を要求する(ステップS2201)。

具体的には、端末装置102のユーザI/F部1208は、メタデータなどを利用して、ユーザが再生したいコンテンツのライセンスIDを取得し、ライセンスIDをICカード103に送信するため、第1のカードI/F部1207に送信する。第1のカードI/F部1207は、受信したライセンスIDをICカード103に送信する。

【0198】

ICカード103は、ライセンスDB1212から該当ライセンスIDを有するライセンスを検索する(ステップS2202)。

具体的には、ICカード103の第2のカードI/F部1213は、受信したライセンスIDをライセンス処理部1217に送信し、ライセンス処理部1217はライセンスIDをキーとして、ライセンスDB1212を検索する。

【0199】

ライセンス処理部1217は、要求されたライセンスIDと一致する、有効なライセンスが存在するか否かを判定する(ステップS2203)。

ステップS2203において、YESである場合、すなわち、有効なライセンスが存在する場合には、ステップS2204を実行する。

【0200】

ステップS2203において、NOである場合、すなわち、有効なライセンスが存在しない場合には、再生不可として、ステップS2205を実行する。

ライセンス処理部1217は、取得したライセンスからコンテンツ鍵と利用条件を取得する(ステップS2204)。

【0201】

具体的には、ライセンス処理部1217は、取得したライセンス1600から、コンテンツ鍵Kc1606と、有効期限1603、再生回数1604、書き出し回数1605を取得する。まず、有効期限1603～書き出し回数1605のコンテンツの利用条件については、ライセンス処理部1217において、有効期限1603と現在時刻との比較により、ライセンスが有効であるか否かを判定する。同様に、再生回数1604および書き出し回数1605については、ここではユーザがコンテンツの再生を要求していることから、再生回数1604を参照し、再生回数1604が0より大であるか否かを判定する。この利用条件判定において、コンテンツ利用可と判定された場合には、ライセンス処理部1217は、コンテンツ再生と同期して端末装置102から受け取る暗号化ECM-Kc1020を復号するため、コンテンツ鍵Kc1606をECM/EMM復号部1214に送信する。コンテンツ鍵Kc1606は、当該コンテンツの再生の間は、ECM/EMM復号部1214において保持される。

【0202】

第2のカードI/F部1213は、端末装置102に対して、ライセンス処理結果のレスポンスを送信する(ステップS2205)。

具体的には、第2のカードI/F部1213は、ライセンス処理部1217による当該ライセンスの検索、および、ライセンスの利用可否判定の結果を取得して、端末装置102の第1のカードI/F部1207に対して、レスポンスとしてその旨を送信する。

【0203】

端末装置102の第1のカードI/F部1207は、ICカード103からのレスポンスを受信して、コンテンツ復号部1205に送信し、コンテンツ復号部1205は当該コンテンツが再生可能かどうかを確認する(ステップS2206)。

【0204】

ステップS2206において、YESである場合、すなわち、コンテンツが再生可能で

ある場合には、ステップ S 2 2 0 7 を実行する。

ステップ S 2 2 0 6 において、NO である場合、すなわち、コンテンツが再生不可である場合には、本コンテンツ利用処理を終了する。

【0205】

蓄積管理部 1 2 0 4 は、蓄積部 1 2 0 3 から該当コンテンツを読み出し、コンテンツ復号部 1 2 0 5 およびコンテンツ利用部 1 2 0 6 が暗号化コンテンツの復号、および、コンテンツのデコードを開始する（ステップ S 2 2 0 7）。

【0206】

蓄積管理部 1 2 0 4 は、蓄積部 1 2 0 3 から該当コンテンツの全 TS パケットを読み出し、コンテンツの再生が終了したか否かを判定する（ステップ S 2 2 0 8）。

ステップ S 2 2 0 8 において、NO である場合、すなわち、コンテンツの再生が継続中である場合には、ステップ S 2 2 0 9 を実行する。

【0207】

ステップ S 2 2 0 8 において、YES である場合、すなわち、コンテンツの再生が終了した場合には、本コンテンツ再生処理を終了する。

分離部 1 2 0 2 は、蓄積管理部 1 2 0 4 が読み出した該当コンテンツから ECM-K c 1 0 2 0 を受け取り、IC カード 1 0 3 に送信する（ステップ S 2 2 0 9）。

【0208】

具体的には、分離部 1 2 0 2 は、該当コンテンツから ECM-K c 1 0 2 0 の PID の TS パケットを取得し、ECM-K c 1 0 2 0 を再構成する。再構成した ECM-K c 1 0 2 0 を、第 1 のカード I/F 部に渡し、第 1 のカード I/F 部 1 2 0 7 が IC カード 1 0 3 に ECM-K c 1 0 2 0 を送信する。なお、ECM-K c 1 0 2 0 に含まれるスクランブル鍵 K s 2 0 1 は数秒おきに更新されるため、本ステップの処理は数秒に 1 回の割合で行う必要がある。

【0209】

IC カード 1 0 3 は、コンテンツ鍵 K c 2 0 5 によって受信した ECM-K c 1 0 2 0 を復号する（ステップ S 2 2 1 1）。

具体的には、IC カード 1 0 3 の第 2 のカード I/F 部 1 2 1 3 が端末装置 1 0 2 の第 1 のカード I/F 部 1 2 0 7 から受信した ECM-K c 1 0 2 0 を、ECM/EMM 復号部 1 2 1 4 に送信し、ECM/EMM 復号部 1 2 1 4 は、保持しているコンテンツ鍵 K c 1 6 0 6 で ECM-K c 1 0 2 0 を復号する。

【0210】

IC カード 1 0 3 は、ECM-K c 1 0 2 0 から取得したスクランブル鍵 K c 2 0 1 を端末装置 1 0 2 に送信する（ステップ S 2 2 1 2）。

具体的には、IC カード 1 0 3 の ECM/EMM 処理部 1 2 1 5 は、復号した ECM-K c 1 0 2 0 からスクランブル鍵 K s 2 0 1 を取得し、第 2 のカード I/F 部 1 2 1 3 を通じて、端末装置 1 0 2 にスクランブル鍵 K s 2 0 1 を送信する。なお、この際に、ライセンス 1 6 0 0 に設定されたコンテンツの利用条件を参照して、スクランブル鍵 K c 2 0 1 を端末装置 1 0 2 に送信するか否かを判定するようにしても良い。

【0211】

端末装置 1 0 2 のコンテンツ復号部 1 2 0 5 は、IC カード 1 0 3 から取得したスクランブル鍵 K s 2 0 1 で、コンテンツをデスクランブルし、コンテンツ利用部 1 2 0 6 がコンテンツをデコードする（ステップ S 2 2 1 0）。

【0212】

具体的には、コンテンツ復号部 1 2 0 5 は、第 1 のカード I/F 部 1 2 0 7 から、IC カード 1 0 3 より取得したスクランブル鍵 K s 2 0 1 を逐次受け取り、コンテンツ復号部 1 2 0 5 に設定する。蓄積部 1 0 3 から読み出したコンテンツの暗号化 TS パケットを、スクランブル鍵 K s 2 0 1 を用いてデスクランブルし、コンテンツ利用部 1 2 0 6 に送信する。コンテンツ利用部 1 2 0 6 は、コンテンツ復号部 1 2 0 5 から受信したデスクランブル後のコンテンツを MPEG デコードし、図示しないモニタなどに出力する。

【0213】

なお、端末装置102のコンテンツ復号部1205やコンテンツ利用部1206、あるいは、ICカード103のECM/EMM復号部1214などにおいて利用条件に基づき、有効期間、累積の利用時間などのコンテンツの利用制御を行うようにしても良い。この場合、ライセンス1600には、対応した利用条件が含まれるものとする。

【0214】

以上、図22を用いて、端末装置102およびICカード103におけるコンテンツ利用処理について説明した。

以上のように、コンテンツ配信システム1に適用したデジタル権利管理システムでは、端末装置で取得したライセンスのIDと有効期限とを、ライセンスの取得履歴として管理し、少なくともライセンスの取得期限までライセンス取得履歴を保持しておくようにしている。そのため、無制限なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立することでき、事業者の権利を十分保護することが可能となる。

【0215】

なお、本発明における実施の形態では、サーバ型放送方式のKc伝送用ECM1100を用いて、放送局101の送出装置から端末装置102およびICカード103に対して、ライセンス1600に設定する情報を配信するようにしたが、これに限られるものではなく、サーバ型放送方式のECM-Kw1000、ECM-Kc1020、EMM900をはじめ、Kc配信用EMMやサーバ型放送方式のTypeIIで用いられるACI (Account Control Information) などに設定するようにしても良い。また、ライセンス1600に設定する情報を配信するのに加え、ライセンス1600とは異なるフォーマットのライセンスを含めて配信するようにしても良いし、ECMやEMMをライセンス1600とは異なるフォーマットのライセンスであると考えられることもできる。

【0216】

また、本発明における実施の形態では、ライセンス1600をICカード103内部に蓄積するようにしたが、ICカード103の記憶容量が大きい場合を考慮して、少なくともライセンス1600の一部を端末装置102に蓄積するようにしても良い。この場合、ライセンス変換により生成したライセンス1600のセキュリティを確保するために、暗号化が必要である。この暗号化においては、例えば、ICカード103固有のマスタ鍵Km252や複数の端末装置102であらかじめ共有している暗号鍵(グループ鍵)、あるいは、図13で示した蓄積暗号鍵Km'1303など、配信時のワーク鍵Kw203とは異なる暗号鍵を用いることにより、ライセンス1600を端末装置102、ICカード103や、これらの集合にバインドするようにしても良い。あるいは、ライセンス変換前のKc伝送用ECM1100などを端末装置102の蓄積部1203にそのまま蓄積するようにしても良い。この際、暗号変換を行わずにそのまま蓄積しても良いし、ワーク鍵Kw203の定期的または不定期の更新に備えるため、ライセンス1600と同様、Kc伝送用ECMの暗号変換を行うようにしても良い。なお、端末装置102およびICカード103において、ライセンスの暗号変換処理を行う場合には、図23に示すように、ICカード103の内部にECM/EMM再暗号化部2301を追加すると良い。

【0217】

また、本発明における実施の形態では、ライセンス変換履歴であるTL1500において、ライセンスID1501を用いて、ライセンス変換を制御する場合の例を示したが、図24に示すように、Kc伝送用ECM2400にECMを識別するためのID(ECM-ID2401)を設けるようにしても良い。この場合、TL1500において、ライセンスID1501に代えて、ECM-ID2401を用いて、ライセンス変換を制御することができる。ただし、ライセンス1600単位のライセンス変換制御ではなく、Kc伝送用ECM1100単位のライセンス変換制御となる。あるいは、TL1500において、ライセンスID1501に加えて、ECM-ID2401を合わせて用いることにより、ライセンス変換を制御するようにしても良い。この場合、異なるKc伝送用ECM11

00に同一ライセンスIDのライセンス1600が含まれるような場合（すなわち、異なるサービスから同一ライセンスを得る場合）や、通信ネットワーク105などから同一ライセンスIDのライセンス1600を取得した場合でも、ライセンス1600を取得した先を区別することができるため、異なるサービスから同一ライセンスを取得したい場合などにおいて、ライセンス変換ができないといった問題を解決することができる。さらに、これらのIDは、ライセンスやKc伝送用ECM1100などを識別可能な情報であればこれに限られるものではないので、ライセンスのハッシュ値、MAC、URIなどを用いるようにしても良い。

【0218】

また、本発明における実施の形態では、Kc伝送用ECM1100のライセンス変換期限1106（TL1500のライセンス変換期限1502）を絶対日時で表現したが、相対日時を設定するようにしても良い。例えば、ライセンス有効期限1108からの相対日時としても良いし、端末装置102でKc伝送用ECM1100を受信した日時からの相対日時などとしても良い。また、変換が許可される終了日時のみである場合の例を示したが、合わせて開始日時を付与するようにしても良い。

【0219】

また、本発明における実施の形態では、ライセンス1600には必ず有効期限1603が設定される場合の例を示したが、図24で示したKc伝送用ECM2400のように、有効期限1603（Kc伝送用ECM2400のライセンス有効期限1108）が無期限であり、Kc伝送用ECM2400にライセンス変換期限が設定されていない場合も考えられる。この場合には、ICカード103のライセンス変換処理部1216がTL1500のライセンス変換期限1502を生成するようにしても良い。ライセンス変換期限1502の生成にあたっては、Kc伝送用ECM2400の受信日時やライセンス変換を行った日時に一定の期間（例えば、1ヶ月など）を加算するという方法などが考えられる。この加算値については、システム固定値として、端末装置102やICカード103で保持しておく方法もあるが、デジタル放送104や通信ネットワーク105などで、放送局101から動的に変更できるようにしても良い。

【0220】

また、本発明における実施の形態では、TL1500には、ライセンスID1501およびライセンス変換期限1502を記載する場合の例を示したが、図25に示すように、TL2500として、事業者ID2501、サービスタイプ2503、購入情報2504、取得ライセンス数2506を合わせて記載するようにしても良い。これによれば、事業者ID2501を記載するようにしているので、ライセンス2502を事業者毎にユニークな値とすることができる。また、サービスタイプ2503を記載するようにしているので、ティアコンテンツに関するライセンス変換履歴に加えて、PPVコンテンツに関するライセンス変換履歴も統合して管理することが可能となる。また、購入情報2504として、PPVコンテンツを購入した日時を合わせて記載するようにしている。また、取得ライセンス数2506を記載するようにしているので、あらかじめシステム固定値として設定されていたり、放送局101からKc伝送用ECM1100などによって、1つのライセンスに関してユーザが取得可能なライセンス数（すなわち、コピー可能なライセンス数）が指定されたりする場合には、取得ライセンス数2506を記録することによって、取得可能なライセンス数を確実に制御することが可能となる。また、取得可能なライセンス数に限らず、それ以外のライセンスの取得に関する条件を管理するようにしても良い。

【0221】

なお、上記で説明したTL2500を用いる場合、サービスタイプ2503、購入情報2504を用いて、同一のPPVコンテンツ（PPVライセンス）を再度購入する場合に、図26に示すようなメッセージをユーザに提示することができる。

【0222】

図26は、ユーザI/F部1208がユーザに提示するウォーニングメッセージの一例を示す図である。モニタ2601に表示されているメッセージ2602は、ユーザがコン

テンツ「神器2」のライセンスを2004/4/15 19:00:00に購入済であるので、同一コンテンツを再購入してもよいか否かをユーザに確認する旨のメッセージを示している。

【0223】

なお、本発明における実施の形態では、ICカード103で、最初にライセンス変換処理を行った端末装置102の端末装置IDを記録しておくことにより、端末装置102とICカード103とをバインドする場合の例を示したが、これに限られるものでなく、コンテンツやライセンスを共有可能な複数の端末装置102およびICカード103からなるドメインと呼ばれる集合を識別するためのドメインIDを、端末装置IDに代えて用いるようにしても良い。

【0224】

また、本発明における実施の形態では、TL1500において、必ずライセンス変換期限1502を管理する場合の例を示したが、Kc伝送用ECM1100にライセンス変換期限1106やライセンス有効期限1108が設定されていないライセンスのライセンス変換履歴に関しては、時限で管理するのではなく、TL1500のレコード数などにより管理し、古いレコードから消去するなど、ハイブリッドな構成とするようにしても良い。

【0225】

また、本発明における実施の形態では、Kc伝送用ECM1100のサービスタイプ1103を参照して、TL1500にライセンス変換履歴のレコードを追加するか否かを決定するようにしたが、Kc伝送用ECM1100に設定されたコンテンツの利用条件（ライセンス有効期限1108、利用可能回数1110、書き出し可能回数1111などがあげられるが、これらに限られるものではない）がステートを有するか否かによって、レコードを追加するか否かを決定するようにしても良い。このため、Kc伝送用ECM1100またはライセンス1600に、ステートを有するライセンスであるか否かの識別情報を設けても良い。例えば、利用条件がステートを有するライセンスのみレコードとして追加し、ステートを有さないライセンスはレコードとして追加しない、などの方法が考えられる。ここで、利用条件がステートを有するとは、主として利用可能回数1110、書き出し可能回数1111などの回数制限の利用条件などがあげられ、ステートを有さない利用条件としては、主として有効期限1108などがあげられる。

【0226】

また、本発明における実施の形態では、TL1500において、新たなライセンス変換履歴のレコードを追加する際に、ライセンス変換期限1502が経過したレコードを削除するようにしたが、定期的にライセンス変換期限1502が経過したレコードを検索して、削除したり、ICカード103が端末装置102から特定のコマンドを受信した場合に、ライセンス変換期限1502が経過したレコードを検索して、削除したりするようにしても良い。また、ライセンス変換期限1502が経過したレコードの削除のための条件を、放送局101から動的に更新できるようにしても良い。さらに、ユーザ指示によって削除させるようにしても良い。

【0227】

また、本発明における実施の形態では、ICカード103の内部でTL1500を管理するようにしたが、ICカード103の記憶容量を考慮して、少なくともTL1500の一部を端末装置102の蓄積部1203において保持するようにしても良い。このとき、蓄積部1203において、悪意あるユーザなどによるTL1500の不正な操作を防止するため、蓄積部1203に保持するTL1500のハッシュ値を、ICカード103で保持する必要がある。また、この場合、ある端末装置102の蓄積部1203にTL1500を蓄積した場合、他の端末装置102で新たにライセンス取得（変換）を行うと、ユーザが取得可能なライセンス数の不整合が生ずる可能性がある。よって、端末装置102にTL1500を蓄積した場合には、当該端末装置102を一意に識別するIDをICカード103で保持することにより、ライセンスを取得可能な端末装置102を限定する必要がある。また、事前にこのような問題を回避するため、最初にライセンスを取得した端末

装置 102 の ID を IC カード 103 で保持しておくことによって、あらかじめライセンスを取得可能な端末装置 102 を限定するようにしても良い。

【0228】

なお、上記のように、ライセンスを取得可能な端末装置 102 を限定する場合、図 27 に示すように、「別端末で既にライセンスを取得しているため、この端末ではライセンスは取得できません。」などのメッセージ (2702) をユーザに提示するようにしても良い。合わせて、ライセンスを取得可能な端末の識別子 (図 27 では、TERMINAL ID-1) を提示するようにしても良い。また、これに限らず、他のカードにライセンスを移動した場合などにメッセージをユーザに提示するようにしても良い。

【0229】

また、本発明における実施の形態では、IC カード 103 単位で TL1500 を管理するようにしたが、IC カード 103 内部で放送局 101 (事業者) 毎に管理するようにしても良い。また、複数の IC カード 103 間で連携することにより、複数 IC カード 103 (ドメイン) 毎で管理するようにしても良い。

【0230】

また、ライセンス変換履歴である TL1500 を、放送局 101 や他の端末装置 102、他の IC カード 103 に送信し、放送局 101 や他の端末装置 102、他の IC カード 103 で利用することもできる。

【0231】

また、IC カード 103 でのライセンス変換処理中において、端末装置 102 の電源断や、IC カードの取り外しなどにより、ライセンス変換完了前に TL1500 のみが残ってしまい、ユーザが不利益を被る場合に備えて、IC カード 103 で一定の回数に限って再取得を許可するようしたり、通信ネットワーク 105 を用いて、放送局 101 と通信を行い、TL1500 を参照しつつ、ライセンス 1600 を再取得できるようにしたりすることもできる。

【0232】

また、本発明における実施の形態では、放送局 101 における送出装置、端末装置 102 を機能ブロックで構成することとしたが、図 17 ~ 図 22 に示したフローチャートを実現するプログラムを CPU、記憶装置、通信装置などからなる汎用のコンピュータ装置で実行することによって、放送局 101 における送出装置や、端末装置 102 を実現するようにしてもよい。

【0233】

また、配信装置および端末装置を構成する各機能ブロックは、複数のシステム LSI などでも実現してもよいし、単一のシステム LSI で実現してもよい。

さらに、本発明における実施の形態では、単一の配信経路からコンテンツやライセンス、制御情報などを取得する場合の例を示したが、デジタル放送とインターネットを併用したり、パッケージメディアとインターネットを併用したりといった、複合的な配信経路から構成されたコンテンツ配信システムに適用することもできる。

【産業上の利用可能性】

【0234】

本発明にかかるデジタル権利管理システムは、端末装置で取得したライセンス ID と有効期限とを合わせてリストで管理し、少なくともライセンスの有効期限までレコードと保持することにより、不正なライセンス取得の防止と、管理するデータサイズの増大の防止とを両立できるという効果を有し、デジタル放送、デジタル CATV、インターネットなどによるコンテンツ配信サービスにおけるデジタル権利管理システムなどとして有用である。またパッケージメディアなどの可搬メディアなどによるコンテンツ配信サービスにおけるデジタル権利管理システムにも応用できる。

【図面の簡単な説明】

【0235】

【図 1】 本発明の実施の形態に係るコンテンツ配信システム 1 の全体の概略構成を示

す図

- 【図 2】本発明の実施の形態に係る暗号スキームの概要を示す図
- 【図 3】本発明の実施の形態に係る放送局 101 の構成を示す機能ブロック図
- 【図 4】本発明の実施の形態に係る契約情報管理 DB 301 の契約情報管理テーブル 400 の構成を示す図
- 【図 5】本発明の実施の形態に係るワーク鍵 DB 302 のワーク鍵管理テーブル 500 の構成を示す図
- 【図 6】本発明の実施の形態に係るコンテンツ属性情報 DB 303 のコンテンツ属性情報管理テーブル 600 の構成を示す図
- 【図 7】本発明の実施の形態に係るコンテンツ鍵 DB 304 のコンテンツ鍵管理テーブル 700 の構成を示す図
- 【図 8】本発明の実施の形態に係るコンテンツ DB 305 のコンテンツ管理テーブル 800 の構成を示す図
- 【図 9】本発明の実施の形態に係る EMM 900 の構成を示す図
- 【図 10】本発明の実施の形態に係る ECM-Kw 1000、ECM-Kc 1020 の構成を示す図
- 【図 11】本発明の実施の形態に係る Kc 伝送用 ECM 1100 の構成を示す図
- 【図 12】本発明の実施の形態に係る端末装置 102 の構成を示す図
- 【図 13】本発明の実施の形態に係るカード管理情報 DB 1210 の共通情報テーブル 1300 の構成を示す図
- 【図 14】本発明の実施の形態に係るカード管理情報 DB 1210 の事業者別情報テーブル 1400 の構成を示す図
- 【図 15】本発明の実施の形態に係る TL 1500 の構成を示す図
- 【図 16】本発明の実施の形態に係るライセンス 1600 の構成を示す図
- 【図 17】本発明の実施の形態に係る放送局 101 における契約処理、端末装置 102 および IC カード 103 における EMM 受信処理を示すフローチャート
- 【図 18】本発明の実施の形態に係る放送局 101 におけるコンテンツ送出処理を示すフローチャート
- 【図 19】本発明の実施の形態に係る端末装置 102 および IC カード 103 におけるコンテンツ蓄積処理を示すフローチャート
- 【図 20】本発明の実施の形態に係るライセンス変換不可時にユーザに提示するメッセージを示す図
- 【図 21】本発明の実施の形態に係る IC カード 103 におけるライセンス変換可否判定処理を示すフローチャート
- 【図 22】本発明の実施の形態に係る端末装置 102 および IC カード 103 におけるコンテンツ利用処理を示すフローチャート
- 【図 23】本発明の実施の形態の変形例に係る端末装置 102 の構成を示す図
- 【図 24】本発明の実施の形態の変形例に係る Kc 伝送用 ECM 2400 の構成を示す図
- 【図 25】本発明の実施の形態の変形例に係る TL 2500 の構成を示す図
- 【図 26】本発明の実施の形態の変形例に係る PPV コンテンツの重複購入検出時にユーザに提示するメッセージを示す図
- 【図 27】本発明の実施の形態の変形例に係る別端末でのライセンス取得済みによるライセンス取得不可時にユーザに提示するメッセージを示す図

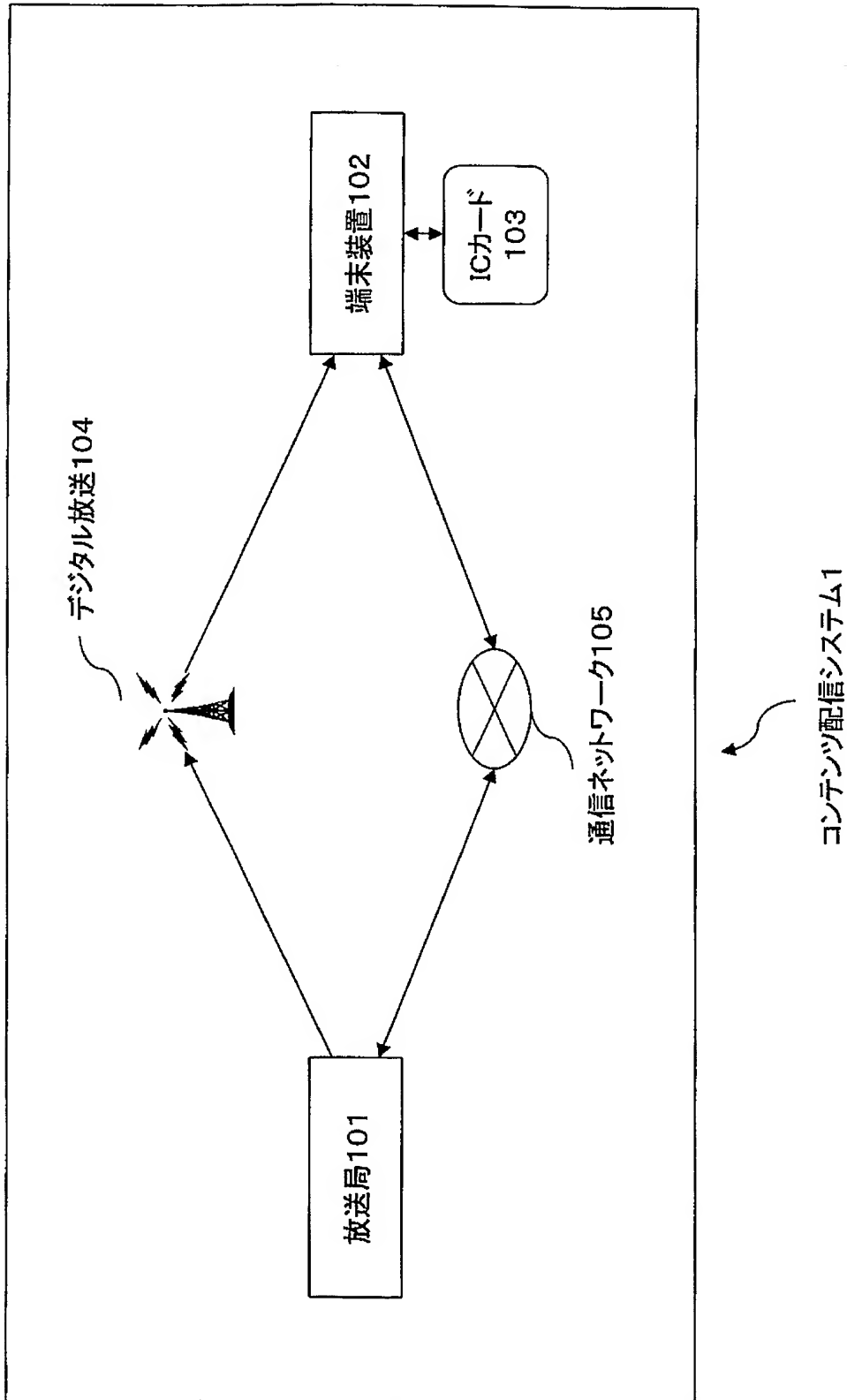
【符号の説明】

【0236】

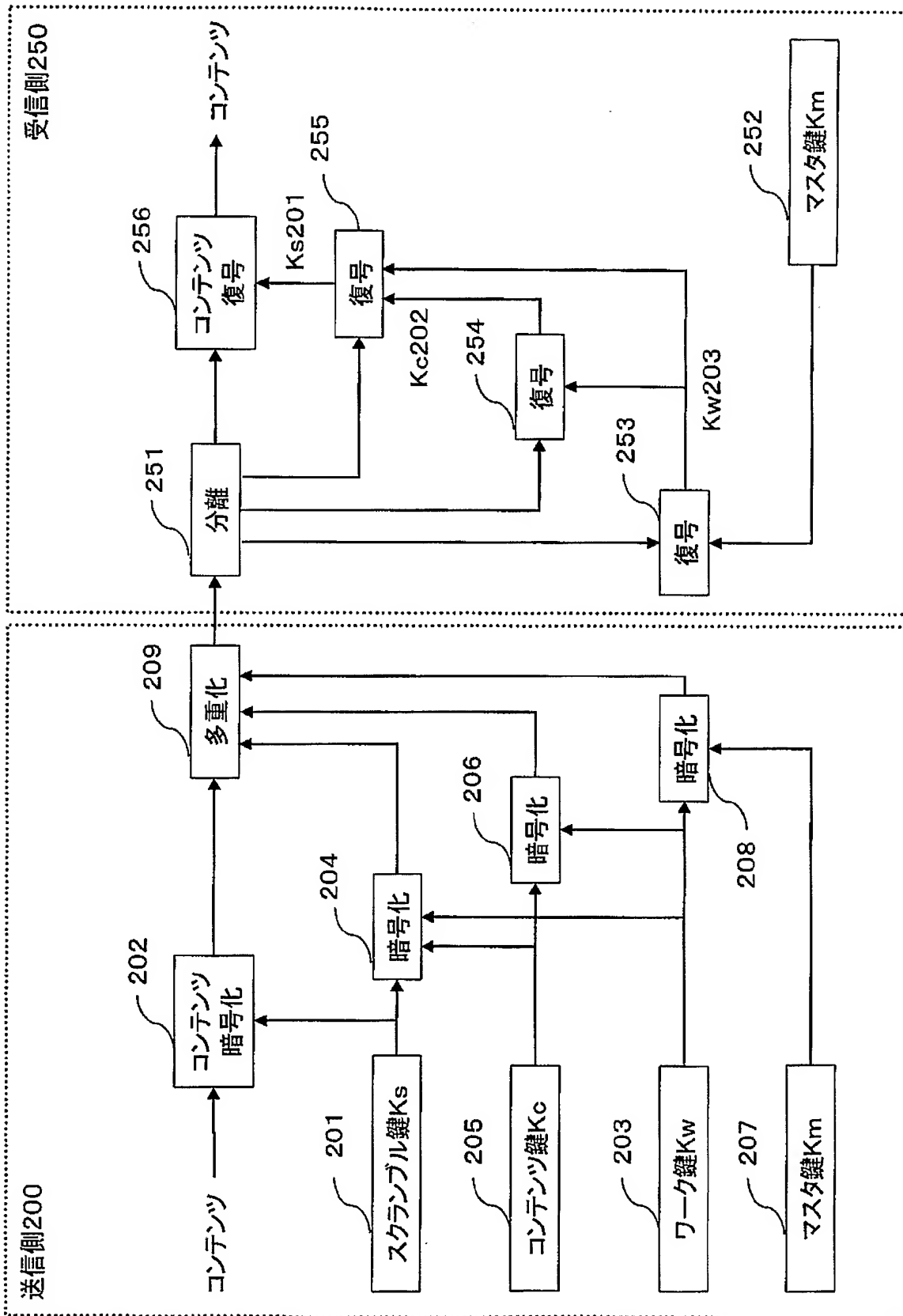
- 1 コンテンツ配信システム
- 101 放送局
- 102 端末装置
- 103 IC カード

1 0 4 デジタル放送
1 0 5 通信ネットワーク
2 0 1 スクランブル鍵 K s
2 0 3、5 0 2、1 4 0 6 ワーク鍵 K w
2 0 5、7 0 3、1 6 0 6 コンテンツ鍵 K c
2 0 7、2 5 2、4 0 6、1 3 0 2 マスタ鍵 K m
3 0 1 契約情報管理 D B
3 0 2 ワーク鍵 D B
3 0 3 コンテンツ属性情報 D B
3 0 4 コンテンツ鍵 D B
3 0 5 コンテンツ D B
3 0 6 通信部
3 0 7 契約処理部
3 0 8 E M M 生成部
3 0 9 E M M 暗号化部
3 1 0 E C M 生成部
3 1 1 E C M 暗号化部
3 1 2 コンテンツ符号化部
3 1 3 多重化部
3 1 4 コンテンツ暗号化部
3 1 5 コンテンツ送出部
9 0 0 E M M
1 0 0 0 E C M - K w
1 0 2 0 E C M - K c
1 1 0 0、2 4 0 0 K c 伝送用 E C M
1 2 0 1 送受信部
1 2 0 2 分離部
1 2 0 3 蓄積部
1 2 0 4 蓄積管理部
1 2 0 5 コンテンツ復号部
1 2 0 6 コンテンツ利用部
1 2 0 7、1 2 1 3 カード I / F 部
1 2 0 8 ユーザ I / F 部
1 2 1 0 カード管理情報 D B
1 2 1 1 変換履歴 D B
1 2 1 2 ライセンス D B
1 2 1 4 E C M / E M M 復号部
1 2 1 5 E C M / E M M 処理部
1 2 1 6 ライセンス変換処理部
1 2 1 7 ライセンス処理部
1 5 0 0、2 5 0 0 T L
1 6 0 0 ライセンス

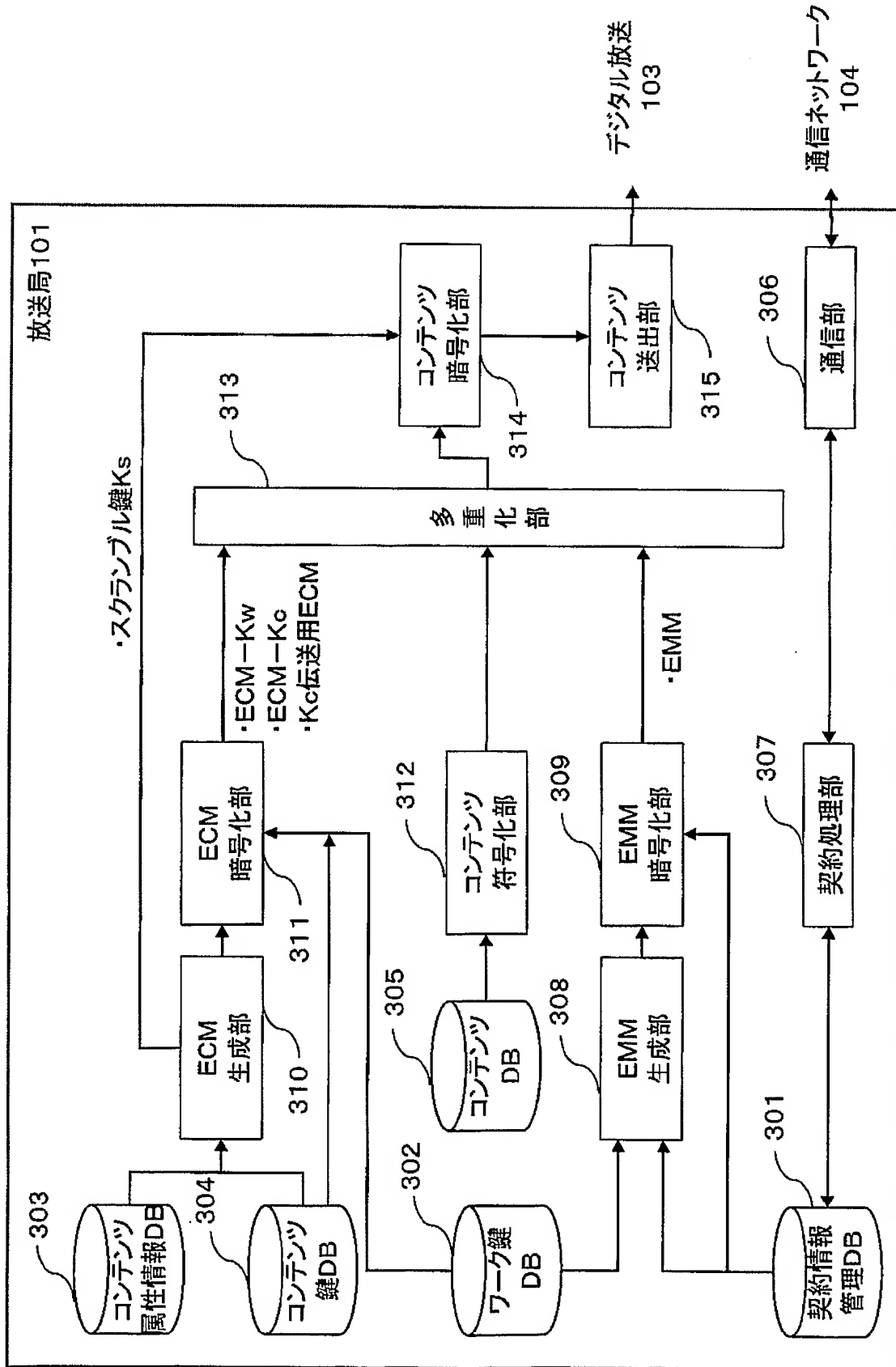
【書類名】 図面
【図 1】



【図 2】



【図 3】



【図 4】

401	402	403	404	405	406
カードID	ティア契約ID	PPV契約ID	有効期限	蓄積暗号鍵Km'	マスタ鍵Km
CARD-ID-1	TIERCONT-ID-1	PPVCONT-ID-1	2004/4/1~ 2005/3/31	0x111...111	0x111...111
CARD-ID-2	TIERCONT-ID-1	PPVCONT-ID-2	2003/12/1~ 2004/11/30	0x222...222	0x222...222
CARD-ID-3	TIERCONT-ID-2	PPVCONT-ID-1	2004/1/1~ 2004/4/30	0x333...333	0x333...333
CARD-ID-4	TIERCONT-ID-3	PPVCONT-ID-1	2004/1/1~ 2005/3/31	0x444...444	0x444...444
...

契約情報管理テーブル400

【図 5】

ワーク鍵ID	ワーク鍵Kw	ワーク鍵利用開始日
WK-ID-1	0x123...cdf	2003/11/24
WK-ID-2	0x001...999	2004/12/20
...

ワーク鍵管理テーブル500

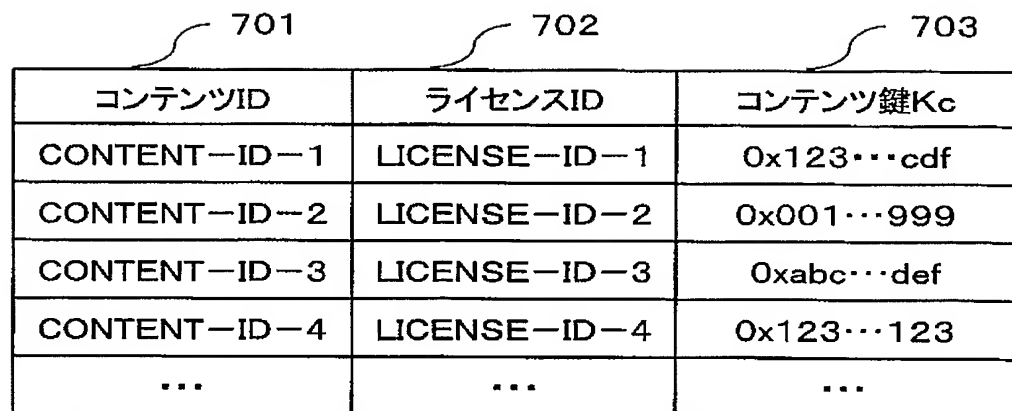
【図 6】

コンテンツID	ライセンスID	利用条件	契約情報	ライセンス 変換期限
CONTENT-ID-1	LICENSE-ID-1	有効期間: 1ヶ月	TIERCONT-ID-1	2004/4/30
CONTENT-ID-2	LICENSE-ID-2	有効期間: 1ヶ月、再生回数: 10回	TIERCONT-ID-1 TIERCONT-ID-2	2004/4/15
CONTENT-ID-3	LICENSE-ID-3	有効期間: 3ヶ月	TIERCONT-ID-1	2004/4/25
CONTENT-ID-4	LICENSE-ID-4	有効期間: 3日、書き出し回数: 1回	PPVCONT-ID-1	2004/5/1
...

コンテンツ属性情報管理テーブル600



【図 7】



701 コンテンツID	702 ライセンスID	703 コンテンツ鍵Kc
CONTENT-ID-1	LICENSE-ID-1	0x123...cdf
CONTENT-ID-2	LICENSE-ID-2	0x001...999
CONTENT-ID-3	LICENSE-ID-3	0xabc...def
CONTENT-ID-4	LICENSE-ID-4	0x123...123
...

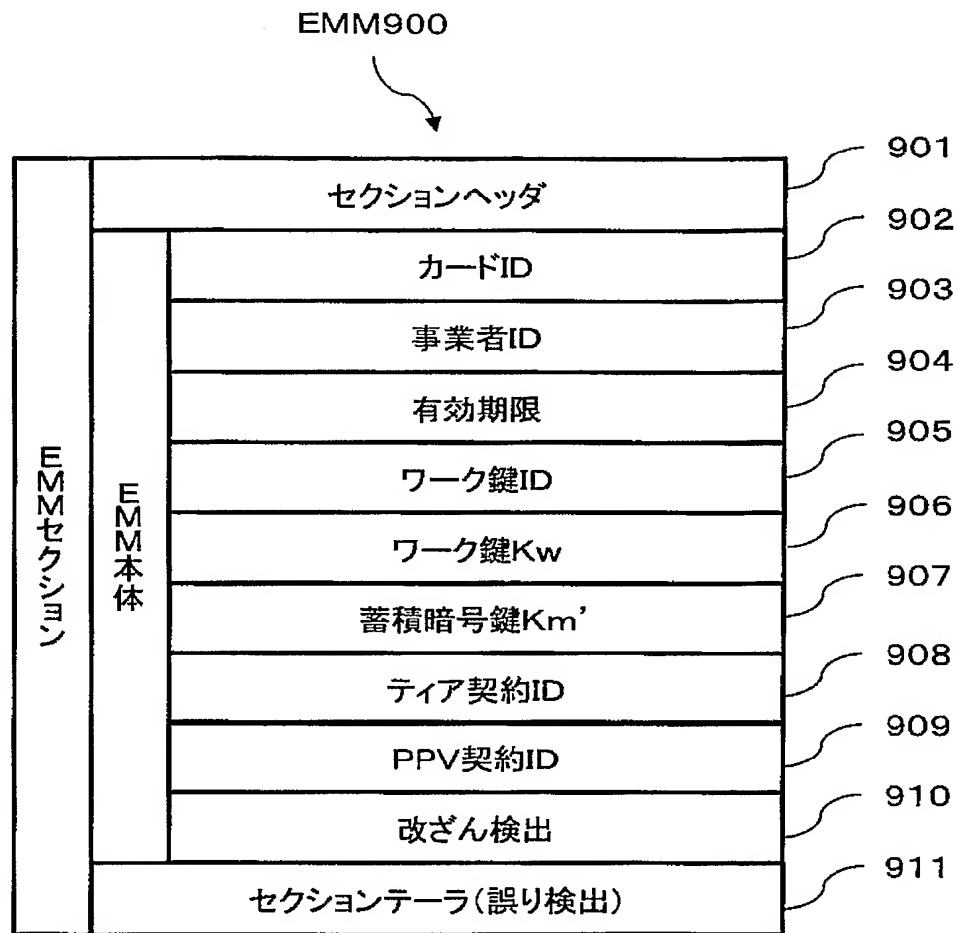
コンテンツ鍵管理テーブル700

【図 8】

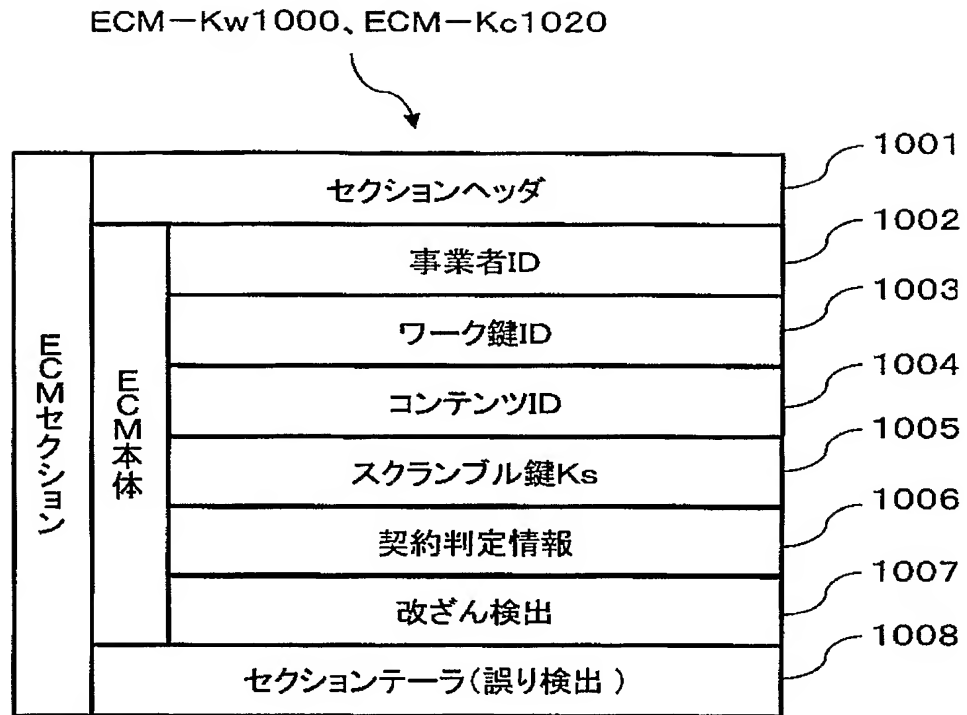
801		802		803		804	
コンテンツID	コンテンツ名称	放送日時	ファイル名				
CONTENT-ID-1	マンデースポーツ	2004/4/8 21:00:00	/SPORT/.../MONSPORTS.VC				
CONTENT-ID-2	GOODBYE13	2004/4/8 22:00:00	/DRAMA/.../GOODBYE.VC				
CONTENT-ID-3	網場の犬	2004/4/10 17:30:00	/ANIME/.../AMIBA.VC				
CONTENT-ID-4	神器2	2004/5/1 19:00:00	/MOVIE/.../JINGI2.VC				
...

コンテンツ管理テーブル800

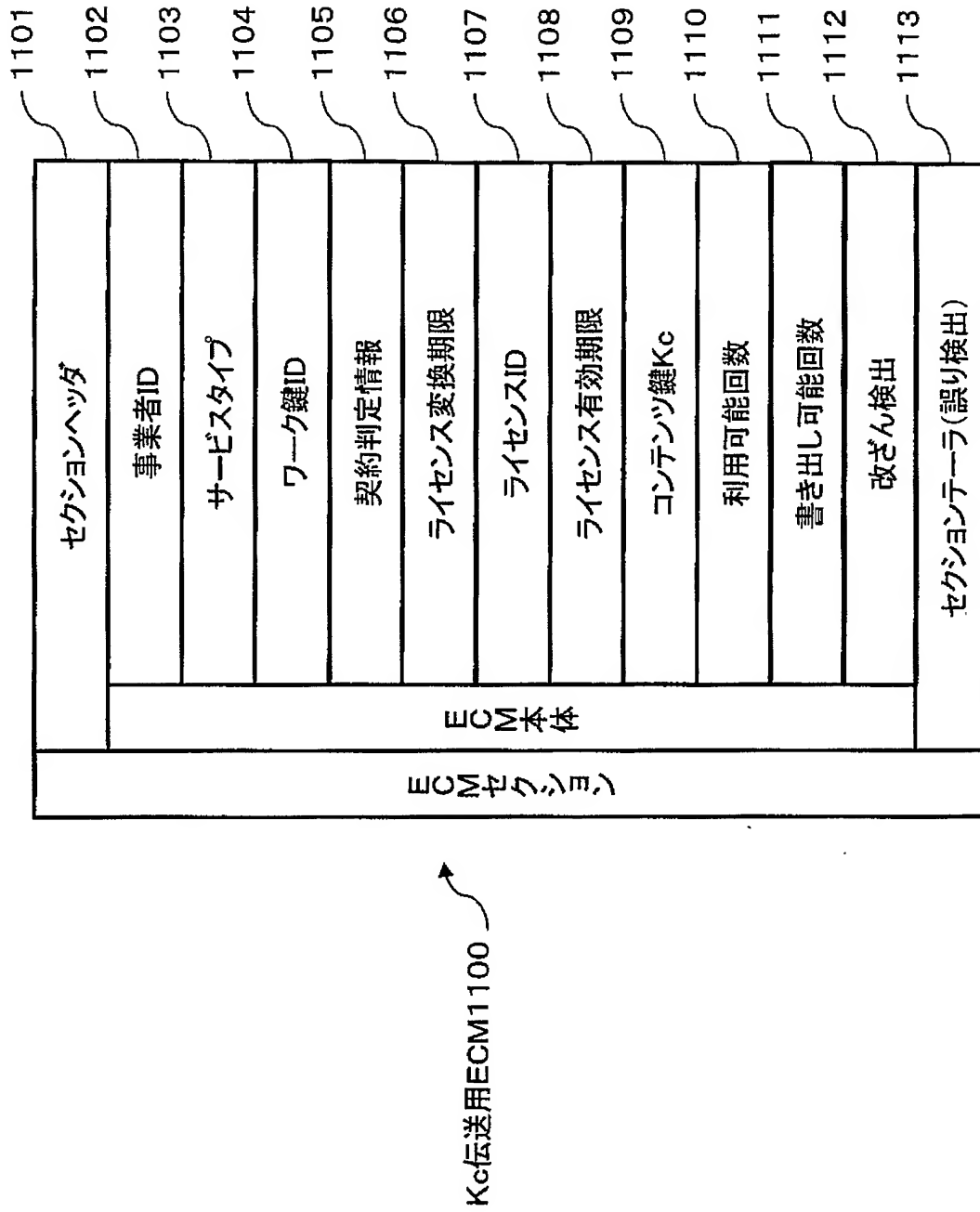
【図 9】



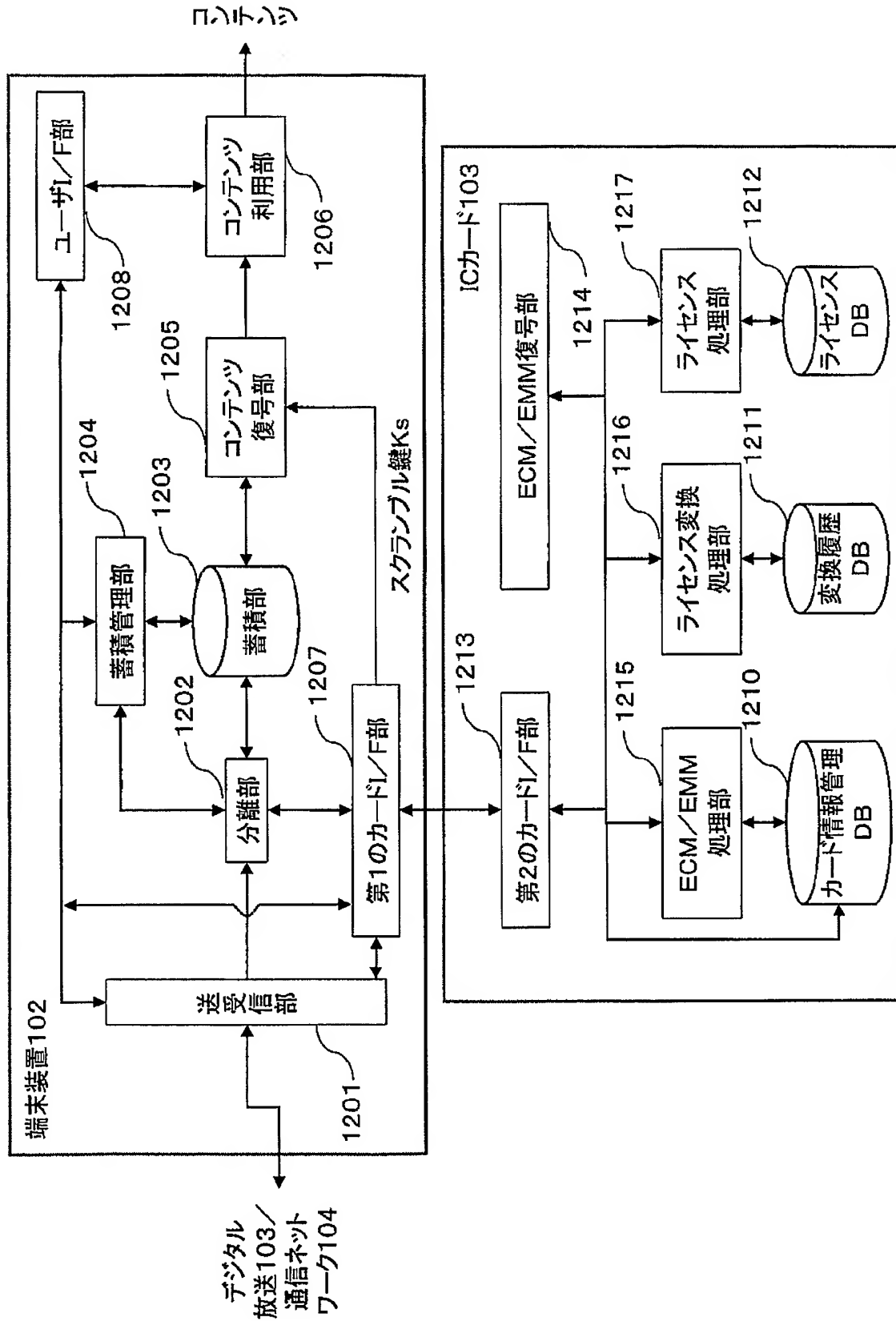
【図 10】



【図 1 1】



【図 12】



【図 1 3】

カードID	マスタ鍵Km	蓄積暗号鍵Km'
0x000...001	0x111...111	0x777...777

共通情報テーブル1300

【図 14】

事業者ID	ティア契約ID	PPV契約ID	有効期限	ワーク鍵ID	ワーク鍵Kw
SERVICE-ID-1	TIERCONT-ID-1	PPVCONT-ID-1	2004/4/1~ 2005/3/31	KW-ID-1	0x111...111
SERVICE-ID-10	---	PPVCONT-ID-1	2004/1/1~ 2005/3/31	KW-ID-1	0x555...555
...

事業者別情報テーブル1400

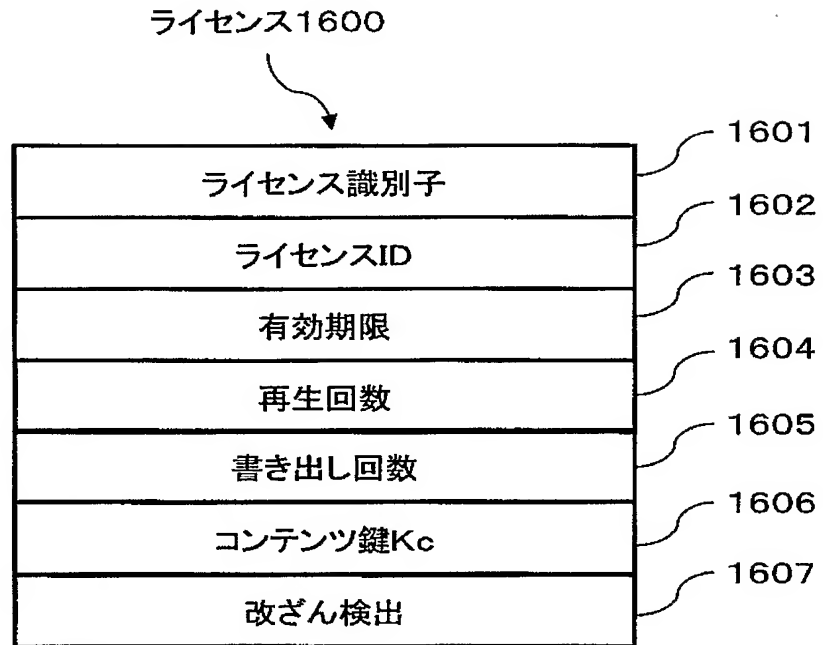
【図 15】

The diagram shows a table with two columns. The first column is labeled 1501 and the second column is labeled 1502. The table contains five rows of data, with the last row containing an ellipsis. An arrow labeled TL1500 points to the bottom of the table.

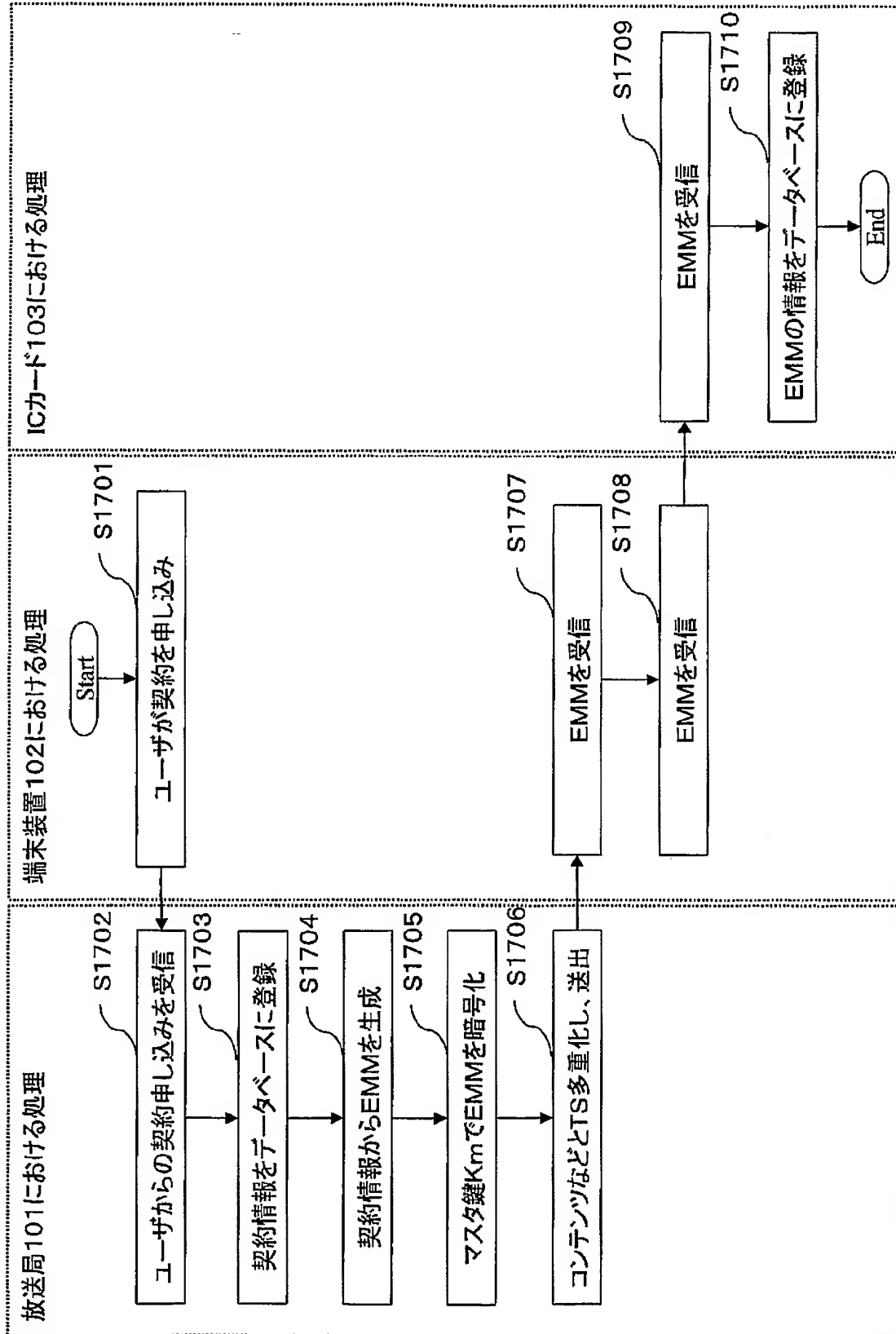
ライセンスID	ライセンス変換期限
LICENSE-ID-1	2004/4/30
LICENSE-ID-2	2004/4/15
LICENSE-ID-3	2004/4/25
LICENSE-ID-4	2004/5/1
...	

TL1500

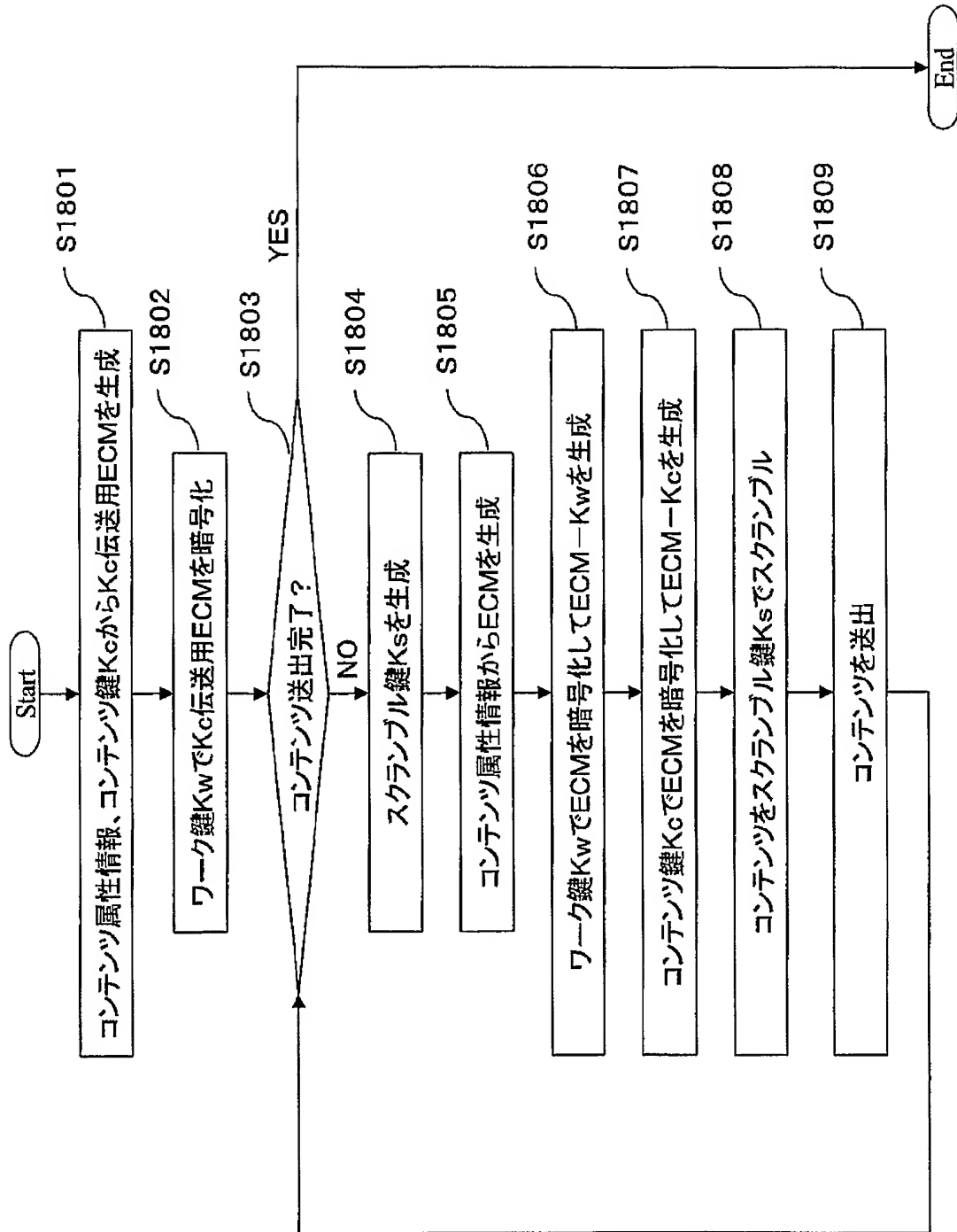
【図 16】



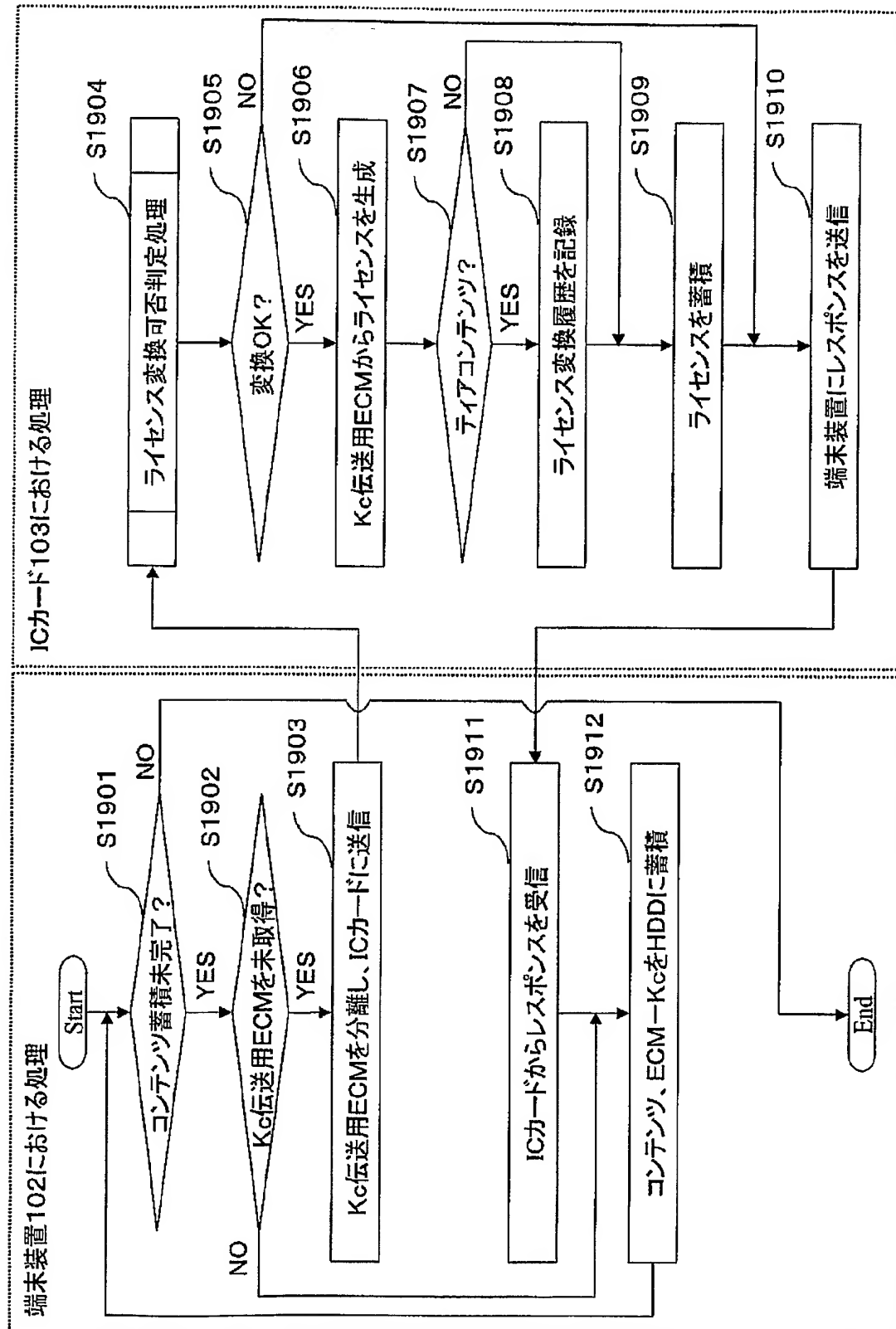
【図 17】



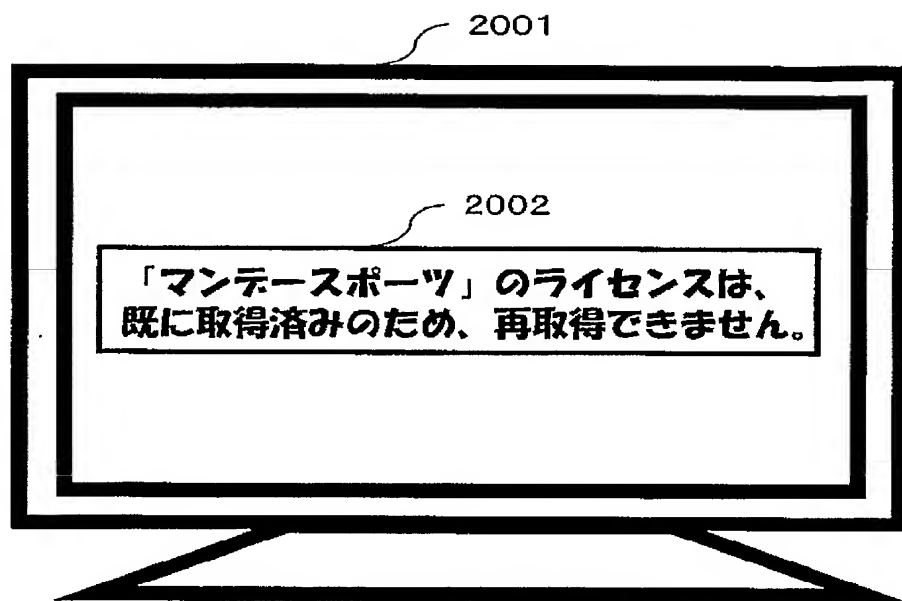
【図 18】



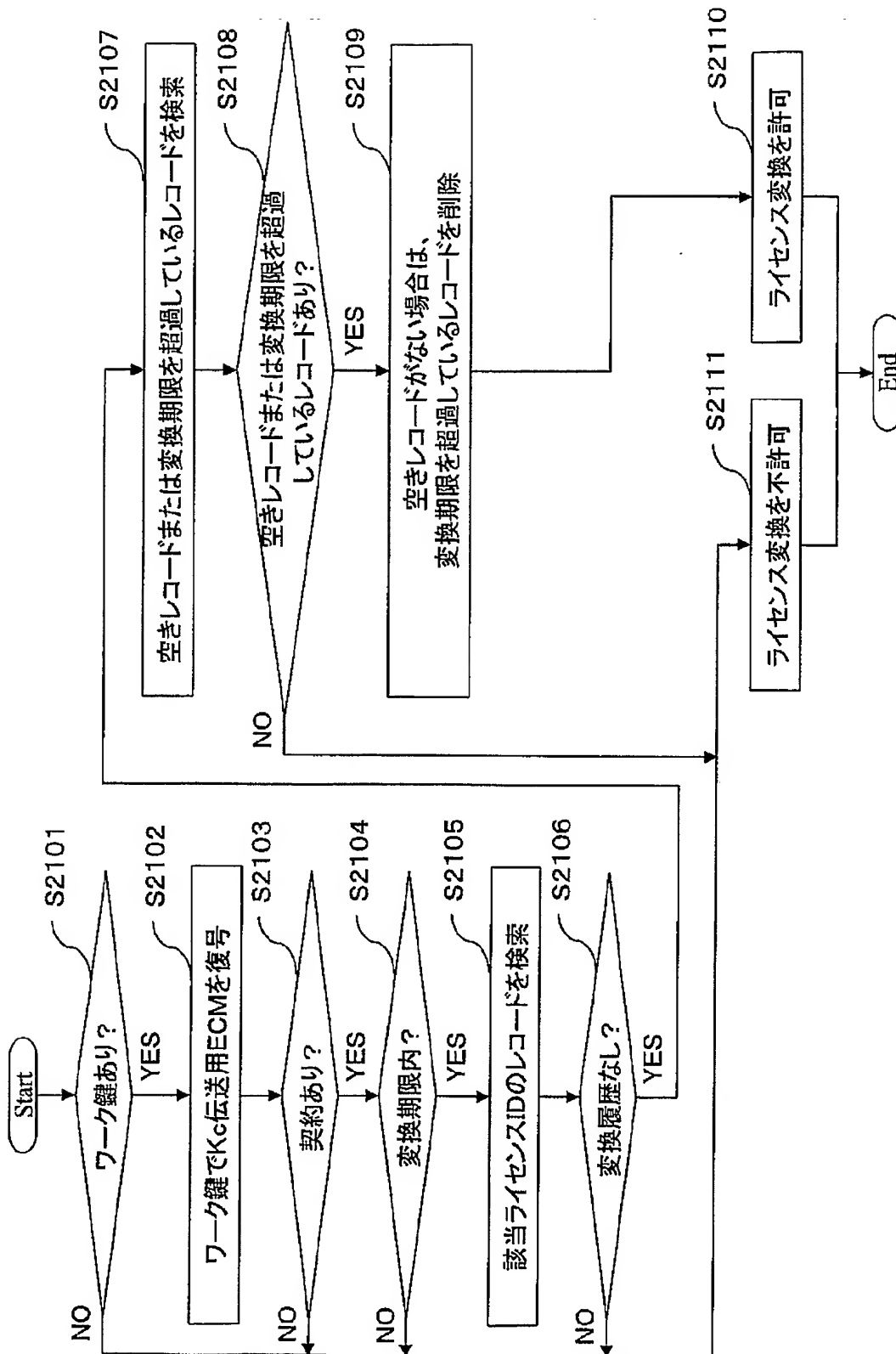
【図 19】



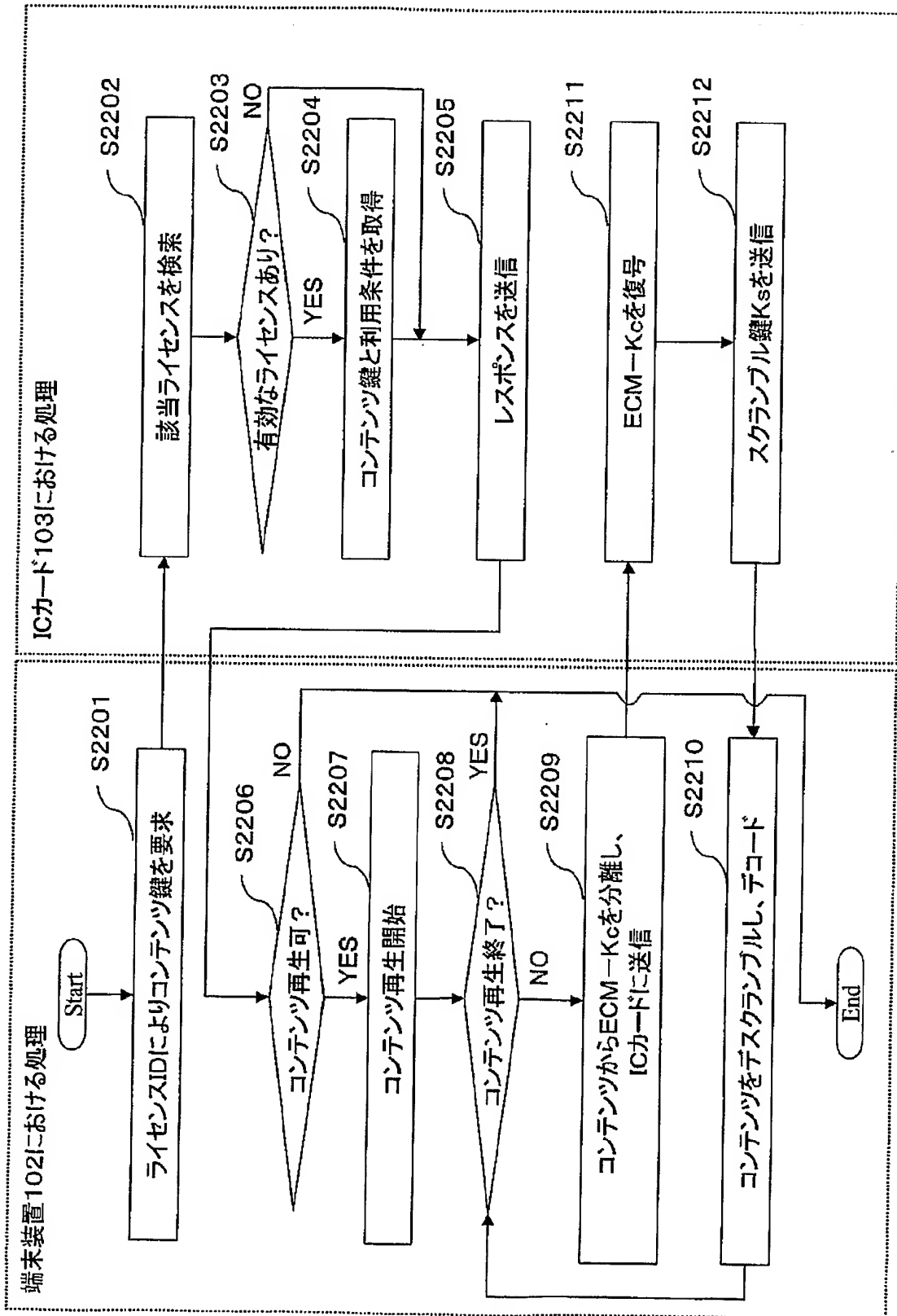
【図 20】



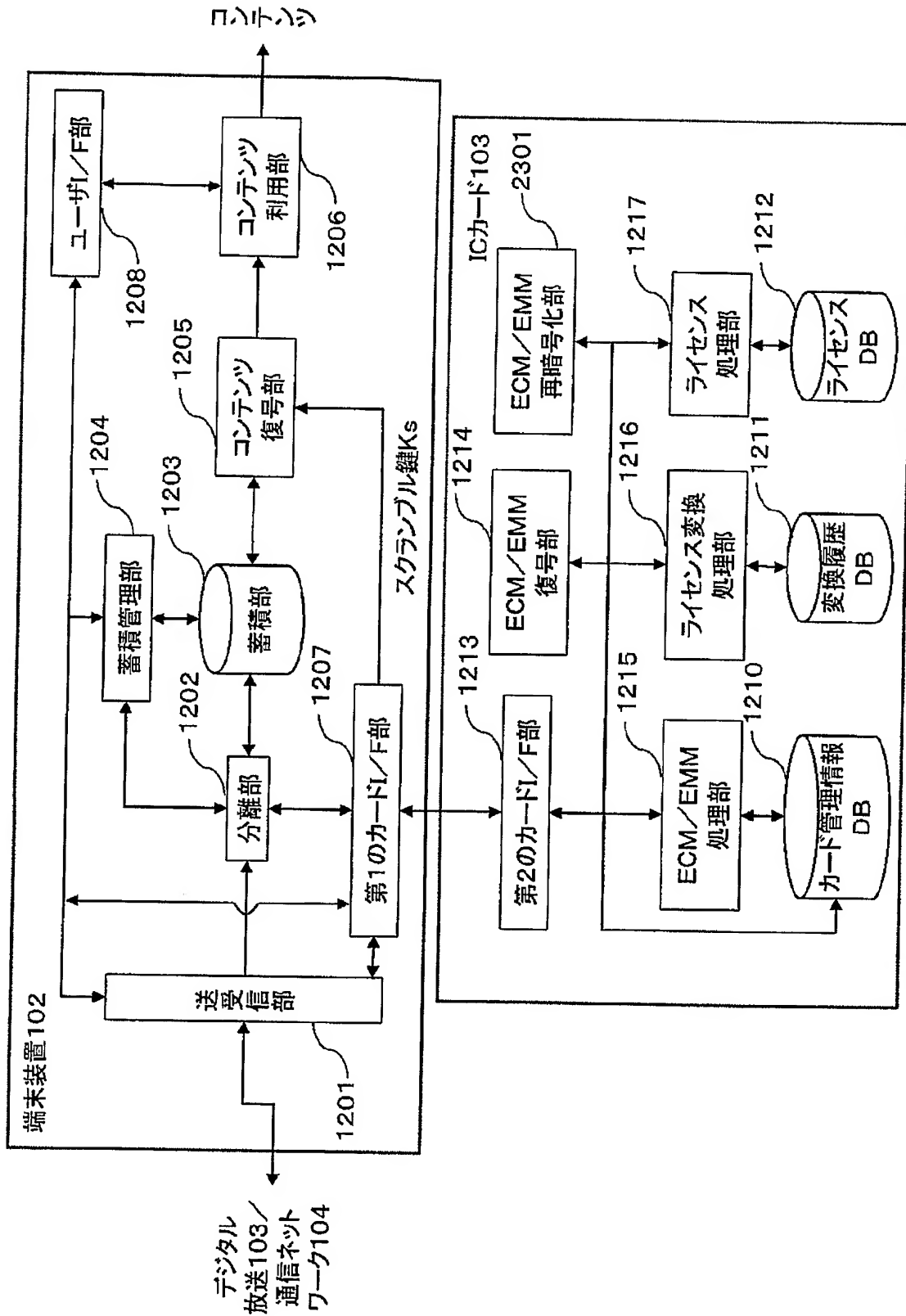
【図 21】



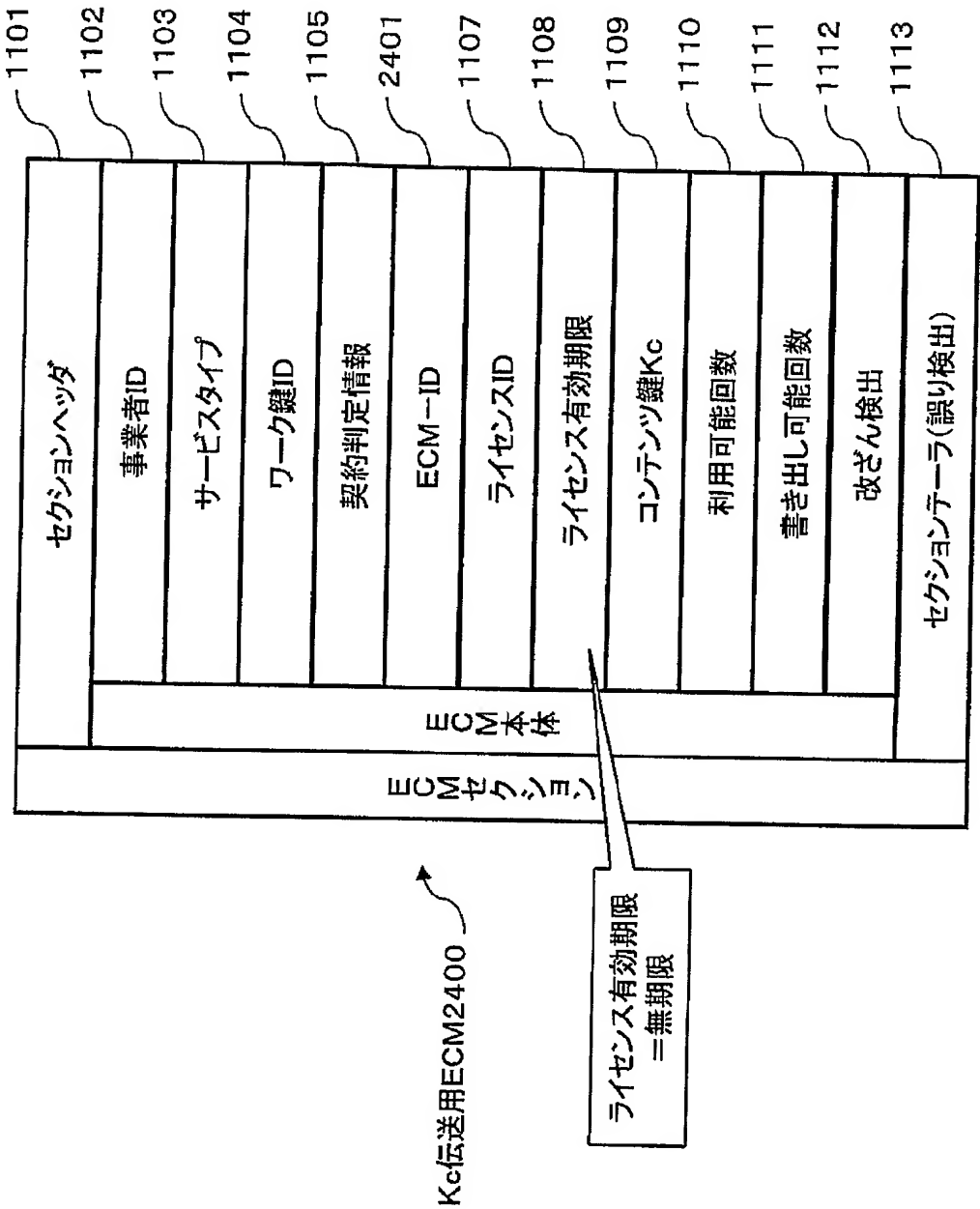
【図 22】



【図 23】



【図 24】

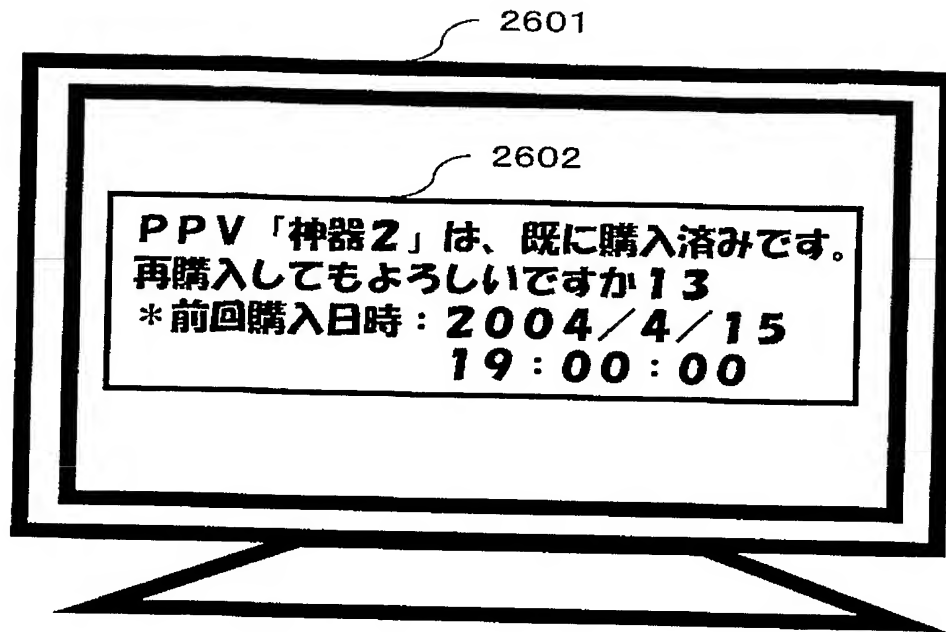


【図 25】

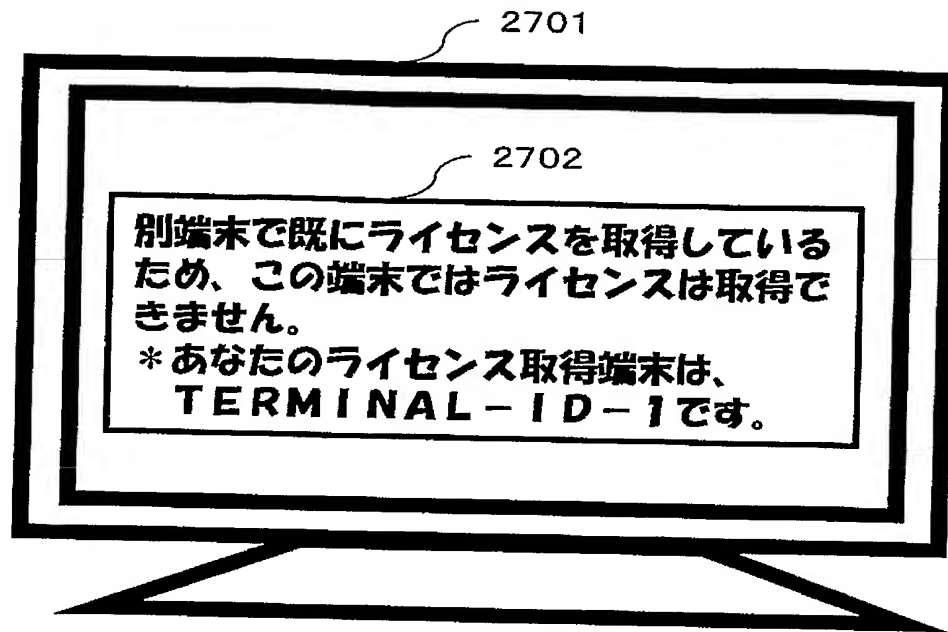
事業者ID	ライセンスID	サービスタイプ	購入情報	ライセンス変換期限	取得ライセンス数
SERVICE-ID -1	LICENSE-ID-1	TIERCONT	-	2004/4/15	2回/3回 (2004/4/14、 2004/4/15)
SERVICE-ID -5	LICENSE-ID-2	TIERCONT	-		
SERVICE-ID -30	LICENSE-ID-3	TIERCONT	-	2004/5/15	
SERVICE-ID -2	LICENSE-ID-4	PPVCONT	購入済み (2004/4/25)		1回/1回 (2004/4/24)
...

TL2500

【図 26】



【図 27】



【書類名】 要約書

【要約】

【課題】 デジタル放送で配信するライセンスの不正取得を抑制し、事業者の権利を保護可能なデジタル権利管理システムを提供する。

【解決手段】 送出装置は、生成するライセンスに I D とライセンス取得期限を付与し、端末装置は、ライセンスに付加されたライセンス I D とライセンス取得期限とを含むライセンス取得履歴を記録する。端末装置は、ライセンスの取得時に既に同一ライセンスを取得している場合は、ライセンスの取得を抑制する。また、ライセンス取得履歴記録手段は、少なくともライセンス取得期限まで保持する。

【選択図】 図 1 2

認定・付加情報

特許出願の番号	特願 2 0 0 4 - 1 0 6 3 3 9
受付番号	5 0 4 0 0 5 4 7 3 1 4
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 6 年 4 月 1 日

<認定情報・付加情報>

【提出日】 平成16年 3月31日

特願 2 0 0 4 - 1 0 6 3 3 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社